2013

Katz on a Hot Tin Roof: Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties

Mary Graw Leary
The Catholic University of America, Columbus School of Law

KATZ ON A HOT TIN ROOF—SAVING THE FOURTH AMENDMENT FROM COMMERCIAL CONDITIONING BY REVIVING VOLUNTARINESS IN DISCLOSURES TO THIRD PARTIES

Mary Graw Leary*

INTRODUCTION

In a world in which Americans are tracked on the Internet, tracked through their cell phones, tracked through the apps they purchase, and monitored by hundreds of traffic cameras, privacy is quickly becoming nothing more than a quaint vestige of the past. This situation has caused courts to analyze, consider, and wrestle with the implications that these technologies have on the Fourth Amendment and on privacy. This national dialogue has recently been re-fueled by the Supreme Court's failure to resolve, shape, or offer meaningful guidance on these issues in its recent opportunities to do so.[1]

In a previous article discussing the intersection of technology and the Fourth Amendment, I proposed a reframing of the issue, suggesting that the problem was more fundamental than previously characterized.[2] Much focus has been on situations in which the government has used a technology to conduct surveillance, but I suggest that the issue is greater than governmental use of modern technologies. That previous article posited that society has reached the point about which Justice Blackmun cautioned in *Smith v. Maryland*—the point at which privacy "expectations [have] been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms."[3] Society finds itself at this juncture not because of *governmental* conditioning, as Justice Blackmun warned, but because of a concept I defined as "commercial conditioning."[4]

That article outlined the Fourth Amendment implications of commercial entities

---

* Associate Professor, The Catholic University of America, Columbus School of Law. Special thanks to Paul Ohm, Ric Simmons, and Thomas Clancy for wise insight; to Rebecca Ryan and Steve Young for tireless research and commentary; to MPL, FML, and CEL for title consultation; and to Julie Kendrick for countless rewrites and boundless patience. Special thanks as well to the patient staff at ACLR for their diligent work.

1. *See* United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding warrantless GPS tracking constitutes a search based on a combination of 18th century trespass law); City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (finding regardless of whether defendant exhibited a reasonable expectation of privacy in text messages sent on a pager provided by his government employer, government's reading of text messages did not violate the Fourth Amendment because it was work-related search).

2. *See* Mary Leary, *The Missed Opportunity of* United States v. Jones: *Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 PENN. J. CONST. L. 331, 333 (2012).

3. *See* Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) (discussed in Leary, *supra* note 2, at 337–38).

4. Leary, *supra* note 2, at 339.

taking information from individuals' digital dossiers or digital footprints and sharing it with others, all without affording the individuals the opportunity to object. This conditioning cripples the current *Katz* approach to establishing a search, necessary to trigger Fourth Amendment protections.[5] First, it strips individuals of the ability to demonstrate subjective expectations of privacy. Second, by creating a climate in which no one has an expectation of privacy, these commercial entities have precluded an individual's ability to establish any privacy expectation that society would find reasonable.[6]

I have argued elsewhere that the most promising solution to this problem is a legislative one.[7] Similar to the "Do Not Call" list, I argued that a commercial entity must give an individual the opportunity to demonstrate an expectation of privacy in his or her information before invading one's digital dossier and publishing the information. Specifically, that proposal called for a legislative requirement that an individual opt into such information disclosure before such a disclosure could be made.[8] This framework of commercial conditioning presents an "upstream" approach to the privacy encroachment, asserting that the more significant threat to privacy is not governmental conditioning, but commercial conditioning.

This Article further develops the concept of "commercial conditioning," and explores not a legislative solution, but possible *judicial* responses to the growing reality of private commercial entities eroding privacy expectations and thereby expanding governmental power. This Article does not focus on the *legality of the commercial activity* (such as online tracking), and does not call for its prohibition. Rather, it accepts for purposes of argument that the political will to disallow the practice legislatively does not exist. The Article instead examines the deleterious effect of these commercial practices on the *Katz* test, and recommends the solution begin from there. This Article seeks to guide the judiciary in analyzing evidence containing certain private information obtained by the government from these commercial entities. Such evidence should be afforded the procedural protections of the Fourth Amendment when the government accesses it, a protection not currently available to this private information. In so doing, this Article focuses on a narrow category of information collection by private commercial entities. This includes two types of information: information taken involuntarily or without meaningful consent (1) by commercial entities with which a consumer directly interfaces (primary party takers), and (2) by unknown third parties with whom consumers do not have a direct relationship (third party takers). It further focuses on the Fourth Amendment implications when the government seeks to access this narrow category of information.

The Fourth Amendment is supposed to provide individuals certain procedural

---

5. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).
6. Leary, *supra* note 2, at 339.
7. *Id.* at 365–66.
8. *Id.* at 366.

protections when the government searches private information: namely, a warrant and probable cause. In the absence of legislation regulating or limiting this data collection (or government access to it), the Fourth Amendment should prevent such data from being obtained by the government without any procedural protections. The sole reason this is not the case under our current Fourth Amendment scheme is because of the role commercial entities have come to play in everyday life. In response, this Article proposes that when the government seeks information previously taken involuntarily from the consumer by a commercial entity (either by primary or third parties) that information should have some Fourth Amendment protections. Information taken involuntarily is information taken from the individual without knowledge or adequate consent. Part I of this Article addresses the data collection—both the factual reality and its legal implications—describing commercial conditioning in more detail. Part II analyzes the precedent for assessing the effect of technology on Fourth Amendment freedoms, as well as scholarship, judicial opinions, and the views of individual justices who address the issue. Part III outlines the proposal to reinvigorate the voluntariness aspect of information disclosure inherent in the *Katz* framework. Finally, the Article outlines why this minor judicial adjustment to current doctrine is supported by the purpose of the Fourth Amendment and its corollary doctrines regarding third party holders of information and state action.

I. THE PROBLEM OF COMMERCIAL CONDITIONING

Many threats to privacy exist, but the most serious threat to Fourth Amendment protection in a modern technological age is not government utilization of advanced surveillance technology.[9] Rather, the threat to Fourth Amendment protections is more fundamental and more "upstream" in the process of accessing private information. The threat arises from commercial entities' ubiquitous use of surveillance technologies to obtain information on individuals and share it with others. Often these "others" are companies seeking the information in order to effectively advertise products to individuals. However, they also include the government when it requests or purchases said information. This threat, referred to in this paper and elsewhere as "commercial conditioning," harms individuals directly (by actually invading *their* privacy) and indirectly (by eviscerating overall Fourth Amendment protections).

A. Commercial Conditioning in Daily Life

Commercial entities often take information from individuals' "digital dossiers" without the voluntary consent of the individuals. In so doing, these entities remove from individuals' lives the precious commodity of a sense of privacy—itself fundamental to true freedom. Professor Solove observes that in recent decades, the

9. This is, of course, not to say that this is not a valid concern and one about which society should be vigilant.

ability to control and share personal information has been transformed.[10] He correctly notes this is possible because one's personal information is amassed by the creation of a "digital dossier," a digital "collection of detailed information about an individual."[11] Palfrey and Gasser build on this concept with their term "digital identity," which is a subset of information "composed of all those data elements that are disclosed online to third parties, whether . . . by [] choice or not."[12] Such information collected by entities can be as private as financial data involving debts, purchases, and transactions; biographical information including race, gender, and age; or more personal information such as health, medicine, sexual orientation, religious affiliation, and income. This information is collected by "companies [that the consumer may] have never established any contact with."[13]

Commercial entities' nonconsensual gathering of this personal information from individuals' digital dossiers is commonplace—so commonplace, in fact, that while many know that their information generally can be collected by entities, they do not know how or exactly when. This Section will outline some of the various technologies, devices, and hardware used by commercial entities to collect private information. In so doing, this Article focuses on two types of data takings. The first is when information is extracted by companies with whom an individual is directly interfacing (primary party taking). The second type includes invasions by third party companies with which an individual has no direct interface (third party taking).

1. Privacy Intrusion Generally

The information within digital dossiers is not only information intentionally disclosed by individuals. It also includes information combined with data collected by entities without consumers' consent.[14] These entities then collate and aggregate data collected online about individual users in ways that can reveal significant information.[15] This collection and aggregation is fueled by the $23 billion American advertising industry that may pay web sites to advertise to their users, and also by a new tracking industry that thrives on the availability of

---

10. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1 (2004).

11. *Id.*

12. JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES, 40 (2008). This article will use the terms "digital dossier" and "digital identity" to refer to the information collected about individuals from their digital activities by commercial entities.

13. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1092 (2002); *see also id.* at 1095 (describing digital dossiers as "digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch").

14. Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 212 (2006).

15. *See* Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, WALL ST. J., Nov. 18, 2010, at A1 (exploring use of personal online information by insurance companies to assess health risks of applicants).

information about individuals that technology collects.[16] Even large companies, which originally resisted the notion of tracking their customers, (think of Google's motto "Do No Evil") cannot resist the financial incentives.[17] The Electronic Frontier Foundation has warned there is a race to learn as much about users as possible, and it involves "Internet giants" such as Google, Facebook, Apple, and Microsoft.[18] That race also includes third party takers who take information from consumers without consumers' consent.

> The most intrusive monitoring comes from what are known in the business as 'third party tracking files' .... The first time a site is visited, it installs a tracking file, which assigns the computer a unique ID number. Later, when the user visits another site affiliated with the same tracking company, it can take note of where the user was before, and where he is now.[19]

As Professors Brenner and Clarke note, "[m]ore than ever before, the details about our lives are no longer our own. They belong to the companies that collect them, and the government agencies that buy or demand them in the name of keeping us safe."[20]

---

16. *See* GINA STEVENS, CONG. RESEARCH SERV., R41756, PRIVACY PROTECTIONS FOR PERSONAL INFORMATION ONLINE 1 (2011); FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 5, 17 (2000), http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf (stating that data collected by advertising networks allows companies to make predictions about consumers' future tastes and needs).

17. Microsoft originally planned to block third party cookies, but internal forces altered this strategy. *See* Nick Wingfield, *Microsoft Quashed Effort to Boost Online Privacy*, WALL ST. J., Aug. 1, 2010, at A1. Google also initially resisted income from tracking, but in 2007 it purchased the tracking company DoubleClick for $3.1 billion and now places several tracking devices on computers with an opt-out provision for users. Jessica E. Vascellaro, *Google Agonizes on Privacy as Ad World Vaults Ahead*, WALL ST. J., Aug. 9, 2010, at A1; *see also* Michael Liedtke, *Judge OKs $22.5M Fine Against Google Over Browser Privacy*, SEATTLE TIMES, (Nov. 16, 2012, http://seattletimes.com/html/businesstechnology/2019699717_googleprivacyfinexml.html (describing court approval of settlement between Consumer Watchdog and Google in lawsuit alleging Google breached privacy of Safari users by bypassing default security settings in Safari browsers).

18. Eli Pariser, *What the Internet Knows About You*, CNN (May 22, 2011), http://articles.cnn.com/2011-05-22/opinion/pariser.filter.bubble_1_personal-data-google-and-facebook-web-sites?_s=PM:OPINION. "Google's deal to purchase DoubleClick for $3.1 billion was just one of many Internet industry acquisitions over the last year. Microsoft bought aQuantive for $6 billion, the Publicis Groupe acquired Digitas for $1.3 billion, Yahoo paid more than $680 million for Right Media, an ad exchange, and AOL is believed to have spent $275 million for Tacoda, an ad network." Louise Story, *F.T.C. Member Vows Tighter Controls of Online Ads*, N.Y. TIMES, Nov. 2, 2007, http://www.nytimes.com/2007/11/02/technology/02adco.html.

19. Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, at W1.

20. Brenner & Clarke, *supra* note 14, at 219. The extent of the invasion was demonstrated convincingly by a series of investigative journalism articles published by the Wall Street Journal, all of which examined the main types of surveillance technologies deployed on individuals from various sources. *See e.g.*, Angwin, *supra* note 19. The series found the most popular fifty websites install on average sixty-four pieces of tracking technology on visitors' computers, often without warning or even disclosure to the visitor. *Id.*; Steve Stecklow, *On the Web, Children Face Intensive Tracking*, WALL ST. J., Sept. 17, 2010, at A1. Some sites installed over 100 pieces of tracking technology. A total of 131 companies installed such data on the Wall Street Journal's sample computer. *Id.* Other studies have produced similar results with regard to the vast amount of tracking. *See, e.g.*, MIKA D. AYENSON ET. AL., FLASH COOKIES AND PRIVACY II: NOW WITH HTML5 AND ETAG RESPAWNING, (July 2011), http://www.futureofprivacy.org/wp-content/uploads/2011/07/Flash%20Cookies%20and%20Privacy%20II

This is not simply an advertising issue, but has other implications. For example, a *Wall Street Journal* investigative series found the data collection practice on the sites most popular with teenagers. Those sites placed over 4,000 tracking devices, which is 30 percent more than the number of tracking devices installed on the overall most popular sites.[21] This occurs despite the fact that collecting such data from youth has legal restrictions. Although federal law requires parental consent to collect the names or other identifiable information from anyone younger than thirteen years old, the taking of this information appears to occur uninhibited.[22] Although the FTC announced expanded rules regulating some collection of information from children through these technologies, the effectiveness and legality of this expansion is in question.[23]

In analyzing this phenomenon, the taking of this information will be divided into two different categories based on the consumer's level of knowledge or voluntary consent to take this information. The first involves situations in which data is appropriated from individuals by an entity with which the individual directly interacts: i.e. primary party takers. The second involves collection by third parties (third party takers) often without the knowledge of the individual at all.

2. *Privacy Intrusions by Primary Party Takers*

There are several examples of privacy intrusions in which individuals directly interface with the intruding entity, and they often occur without any knowledge on the part of the user.

%20Now%20with%20HTML5%20and%20ETag%20Respawning.pdf (stating that "[Of] 5,600 standard HTTP cookies on popular sites, over 4,900 were from third parties. Google-controlled cookies were present on 97 of the top 100 sites, including popular government websites . . . . Flash cookies were present on 37 of the top 100 sites").

21. Stecklow, *supra* note 20.

22. *See* 15 U.S.C. § 6502 (2006) (prohibiting websites targeted towards children from collecting personal information from all users and websites with actual knowledge that a particular user is a child from collecting personal information). "Facebook prohibits children under 13 from signing up for its services, but studies have repeatedly shown that millions of under-age children do so anyway, often with help from their parents." Somini Sengupta, *Facebook Says Child Privacy Laws Should Not Apply to 'Like' Buttons*, N.Y. TIMES (Oct. 1, 2012, 6:37 PM), http://bits.blogs.nytimes.com/2012/10/01/facebook-says-child-privacy-laws-should-not-apply-to-like-buttons/.

23. *See* FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1-312.12 (2000) (discussing amendments to Children's Online Privacy Protection Rule); FTC, DISSENTING STATEMENT OF COMMISSIONER MAUREEN K. OHLHAUSEN *in* THE 2010 CHILDREN'S ONLINE PRIVACY PROTECTION ACT RULE REVIEW, www.ftc.gov/os/2012/12/121219copparulesstatement.pdf (arguing that recent amendments to the Children's Online Privacy Protection Act exceed the rulemaking authority of the FTC); Donna Tam, *Children's Privacy Law Catches on to Apps, Social Networks*, CNET (Dec. 19, 2012 12:13 PM), http://news.cnet.com/8301-1009_3-57560037-83/childrens-privacy-law-catches-on-to-apps-social-networks/ (noting only companies that specifically and knowingly target children would be subject to amended rule); Natasha Singer, *New Online Privacy Rules for Children*, N.Y. TIMES, Dec. 19, 2012, at B8 (explaining that new rule significantly expanded the types of companies required to obtain parental consent to obtain information from child visitors to their sites).

a. Computer based intrusion

The classic example is a "cookie," which is a small text file "that can, among other things, be used to help track people's activities online to show them ads targeted to their interests."[24] Not all of these track a user's activities, however. The original purpose of cookies was user convenience, as they allowed the consumer's computer to remember facts such as content of shopping carts, log-in information,[25] or the user's password upon his return to a website.[26] However, as time progressed, primary party and third party takers utilized cookies in more expansive and intrusive ways (to count individuals' visits to networks or web sites, or to track them more substantially).

Flash cookies have a similar history. Their original purpose was also user convenience, but this evolved into one of data collection. Originally they were meant to remember an individual's preferences (such as volume settings) for viewing online videos using the Adobe Flash Player system.[27] Similar to traditional cookies, these flash cookies store data regarding a user's online activities. However, they are nefarious because they store themselves in a different place on the computer than do traditional cookies. As a result, when an individual deletes the cookies on his computer automatically or manually (as part of a privacy protection process), these cookies may not be deleted.[28] In fact, they can be used to re-install regular cookies the user already deleted.[29] Therefore, not only does this technology attach to a user's computer, track his activity on the Internet, and compile more information of one's digital dossier—it also actively precludes the ability of the user to prevent its continued tracking.

Such tracking is not limited to retail web sites. Tracking devices are also utilized by web browsers (which are necessary to merely access the Internet),[30] and search

---

24. Vascellaro, *supra* note 17; *see also, IT Glossary*: *Cookie*, GARTNER, INC., http://www.gartner.com/it-glossary/cookie (last visited Apr. 18, 2013) (defining "cookie" as "a permanent code placed in a file on a computer's hard disk by a website that the computer user has visited. The code uniquely identifies, or 'registers,' that user and can be accessed for [a] number of marketing and site-tracking purposes").

25. Angwin, *supra* note 19.

26. Nick Wingfield, *supra* note 17; *see also*, *WebWise*: *Cookies*, BBC, http://www.bbc.co.uk/webwise/a-z/c/ (defining "cookies" as "small files automatically downloaded to your computer by websites, which can contain information about you and what you've done on that website for the website to view next time you go online").

27. Angwin, *supra* note 19; Stevens, *supra* note 16 at 1; *Online Profiling*, *supra* note 16, at 17 (citing definition of "flash cookie" in FTC staff report); Ayenson et al., *supra* note 20 at 2 (July, 2011), ("Flash cookies, technically called 'local shared objects,' are files used by Adobe Flash developers to store data on users' computers.").

28. STEVENS, *supra* note 27; *see also* Ayenson et. al., *supra* note 20, at 2 (explaining the advantages of Flash cookies relative to HTTP cookies for advertisers to use in tracking consumers).

29. Angwin, *supra* note 19.

30. Gartner Inc. defines "browser" as: "A software program used to locate and display information on the Internet or an intranet. Browsers are most often used to access Web pages. Most can display graphics, photographs and text; multimedia information (e.g., sound and video) may require additional software, often referred to as 'plug-ins.'" *IT Glossary: Browser*, GARTNER, INC., http://www.gartner.com/it-glossary/browser/. A "web browser" is: "The application program that serves as the primary method for accessing the World Wide Web . . . All

engines[31] (which are also indispensable in using the Internet and World Wide Web). These entities can collect data about an individual's activities on their web site, and also "about websites people visit," in order to "track and show them ads across the Internet."[32] In the *Wall Street Journal* study, Google's tracking device was present on 80 percent of the web sites visited. After Google's purchase of the web tracking company DoubleClick, "every page where Google sold a display ad began installing a DoubleClick cookie on users' computers."[33]

With so many companies providing services across different spectrums, the privacy invasion can be significant and unknown to even the savviest consumer. It can lead to a privacy invasion not only by primary party takers, but also affiliated entities. For example, in 2010 the FTC settled with Google charges alleging Google violated the privacy rights of Gmail users when it created Google Buzz, a social networking service.[34] Google offered Google Buzz to Gmail users, and enrolled them even when the users declined. The FTC alleged Google users were not "fully informed regarding the extent their personal information might be shared with, or exposed to, Google users outside of their own personal network."[35]

b. Cell phones and mobile devices

This form of commercial conditioning is not limited to activity on the World Wide Web: the history of cell phone tracking is similar to that of cookies. In an effort to enhance 911 wireless services, the Federal Communications Commission required American cell phone manufacturers to equip most phones with technology that would allow the phone to be traceable.[36] The purpose behind this was to enhance the ability to locate individuals in emergencies.[37] Commercial entities soon realized other uses for GPS tracking, such as the ability to record texts, record GPS location at all times, and access other call details.[38] These services sometimes require software to be downloaded physically to the phone. However, other such

---

browsers include bookmarks (Favorites) that store the addresses (URLs) of frequently used pages." *Encyclopedia: Web Browser*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,1237,t=Web+browser&i=54278,00.asp (last visited Apr. 18, 2013). Common browsers include Internet Explorer, Firefox, Chrome, and Safari. *Id.*

31. A search engine is "a Web site that maintains an index and short summaries of billions of pages on the Web, Google being the world's largest. Most search engine sites are free and paid for by ads." *Encyclopedia: Web Search Engine*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0%2C1237%2Ct%3DWeb+search+engines&i%3D54339%2C00.asp (last visited Apr. 18, 2013).

32. Vascellaro, *supra* note 17.

33. *Id.*

34. *See In re* Google, Inc., No. 102-3136 (F.T.C. filed Mar. 30, 2011), http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

35. STEVENS, *supra* note 27, at 9.

36. 47 C.F.R. § 20.18(g)(v) (2011).

37. Interconnected VoIP Service; Wireless E911 Location Accuracy Requirements; 3911 Requirements for IP-Enabled Service Providers, 76 Fed. Reg. 59916 (Sept. 28, 2011) (to be codified at 47 C.F.R. pt. 20).

38. Justin Scheck, *Stalkers Exploit Cellphone GPS*, WALL ST. J., Aug. 4, 2010, at A1; *see also*, AT&T FamilyMap, *How it Works*, https://familymap.wireless.att.com/finder-att-family/helpContent.htm?topic=1 (de-

systems are provided by the cellular carrier and are activated remotely by companies.[39] While these services began without a nefarious purpose, such as AT&T's FamilyMap feature, police do not need warrants to obtain such detailed tracking information.[40] "Federal law says carriers may comply with such requests, and law-enforcement agencies have pressured them to maintain the tracking systems."[41]

Cell phones and other mobile devices can facilitate threats to privacy in addition to those associated with GPS capabilities. A significant portion of tracking is accomplished through users downloading mobile applications ("Apps") to such devices, which are small pieces of software that allow the device to play games or perform certain functions.[42] With the advent of smartphones, apps were a $6.7 billion industry in 2010.[43] Many of them have no terms of service or privacy agreements, and they remain fairly unregulated. While Apple and Android claim to screen them, many apps have been found to surreptitiously function as information collectors.[44] The Wall Street Journal found many commercial entities use apps to gather identifying information from the phones, combine it with their own databases, and then sell the information.[45] Many of the most popular apps

---

scribing the A-GPS (Assisted GPS) technology and cell tower information used to provide most accurate locations of family members, usually within a few hundred yards to a few miles of the phone's actual location).

39. *Id.*

40. Peter Maass & Megha Rajagopalan, *That's No Phone. That's My Tracker*, N.Y. TIMES TECHNOLOGY BLOG, (July 13, 2012), http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html?_r=0 (reporting that "cellphone carriers responded 1.3 million times last year to law enforcement requests for call data . . . [and] [m]any police agencies don't obtain search warrants when requesting location data from carriers").

41. Scheck, *supra* note 38; *see also* FCC, E-9-1-1 MANDATE (May 26, 2011), http://transition.fcc.gov/pshs/services/911-services/enhanced911/archives/factsheet_requirements_012001.pdf (outlining the FCC's new requirements to provide more precise location information to Public Safety Answering Boards, or PSAP's).

42. *See* Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WALL ST. J., Oct. 17, 2010, at A1 (detailing Facebook's difficulties in restraining popular apps from harvesting and using users' privacy data).

43. Scott Thurm & Yukari Iwatani Kane, *What They Know: A* Wall Street Journal *Investigation: Your Apps Are Watching You*, WALL ST. J., Dec. 17, 2010, at C1. Gartner Inc. states that by 2015, "mobile application development projects targeting smartphones and tablets will outnumber native PC projects by a ratio of 4-to-1 . . . particularly where mobile capabilities can be integrated with location, presence and social information to enhance the usefulness." Eric Savitz, *The Road Ahead: Gartner's Outlook For 2012 and Beyond*, FORBES, (Dec. 1, 2011), http://www.forbes.com/sites/ericsavitz/2011/12/01/the-road-ahead-gartners-outlook-for-2012-and-beyond.

44. *See* Hiawatha Bray, *Smartphone Apps Track Users Even When Shut Down*, THE BOSTON GLOBE, Sept. 2, 2012, at B5 (revealing that "some smartphone apps collect and transmit sensitive information stored on a phone, including location, contacts, and Web browsing histories, even when the apps are not being used by the phone's owner . . . ."); Brian X. Chen, *Why and How Apple Is Collecting Your iPhone Location Data*, WIRED (April 21, 2011), http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking/; Brian X. Chen, *iPhone Tracks Your Every Move, and There's a Map for That*, WIRED (April 20, 2011), http://www.wired.com/gadgetlab/2011/04/iphone-tracks/.

45. *See* Steel & Fowler, *supra* note 42; *see also* Declan McCullagh, *Verizon Draws Fire for Monitoring App Usage, Browsing Habits*, CNET (October 16, 2012), http://news.cnet.com/8301-13578_3-57533001-38/verizon-draws-fire-for-monitoring-app-usage-browsing-habits/ (reporting "'we're able to view just everything that they do,' Verizon Wireless executive has boasted. Privacy groups say initiative—including linking databases showing whether customers own pets—may violate wiretap law").

transmit identifying and sensitive information as well as contacts, web broadcasting history, and location, even when the phone is not being used.[46] This essentially provides access to individual's names (and possibly friends' names) to internet tracking companies.[47] The type of information taken can include important and unique phone identification information and location data.[48] Litigation has alleged apps downloaded from Apple obtained identifying information without the consent of the owners.[49]

The risk to privacy results not only from software, but also from the hardware individuals purchase. Here again, the individual has little opportunity to demonstrate an expectation in privacy. The dramatic increase in cell phone usage[50] has lead to what Professor Paul Ohm refers to as the "one device" issue. The use of one device to communicate leads to one device which tracks location, lists a calendar and friends, tracks phone calls, and stores both sides of a texting exchange on each "endpoint and on network servers in the middle."[51] The one device "coaxes us to communicate through it, and then creates archives of what we say by default."[52] This technology leads to the phone companies themselves threatening privacy. They now collect information about their own customers, "anonymizing" it and selling it to potential buyers.[53]

---

46. Bray, *supra* note 44.

47. Steel & Fowler, *supra* note 42; *see also* Bray, *supra* note 44 ("Angry Birds uses the phone's GPS and Wi-Fi wireless networking features to track the owner's location, even when he's not playing the game, for example. Another game, Bowman, collects information from the phone's Internet browser, including what websites the owner has been visiting. And WhatsApp, a popular text-messaging program, scans the user's address book when it is seemingly idle.").

48. Seungyeop Han et. al., *A Study of Third-Party Tracking by Mobile Apps in the Wild*, UNIVERSITY OF WASHINGTON TECHNICAL REPORT (March 1, 2012), ftp://ftp.cs.washington.edu/tr/2012/03/UW-CSE-12-03-01.PDF (finding that privacy threats are heightened on mobile devices "because they contain a wealth of sensor data and personal information that may be used to profile users . . . includ[ing] where users are and have been, their phone numbers and contacts, call and email histories, photos, and calendar events" and that "some apps do collect and send this information to third parties"); *see also* Maass & Rajagopalan, *supra* note 40 (detailing the explosive development of tracking technology in recent years).

49. *See In re* iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012) (consolidating several actions challenging the propriety of mobile tracking technology).

50. Cell phones are a necessity in American life, with over 85% of people owning one. *See* Maeve Duggan & Lee Rainie, *Cell Phone Activities 2012*, PEW INTERNET & AMERICAN LIFE PROJECT (Nov. 25, 2012), http://pewinternet.org/Reports/2012/Cell-Activities.aspx (finding "fully 85% of American adults own a cell phone and now use the devices to do much more than make phone calls"). Mobile capabilities increase dramatically with each year, and now over 45% of adults own smartphones, and nearly two thirds of all young adults do as well. *See Smartphone Research: Infographic*, PEW INTERNET & AMERICAN LIFE PROJECT (Sept. 17, 2012), http://pewinternet.org/Infographics/2012/Our-Smartphone-Habits.aspx.

51. Paul Ohm, *The Fourth Amendment in A World Without Privacy*, 81 MISS. L.J. 1309, 1315 (2012).

52. *Id.*

53. *See* Kashmir Hill, *Verizon Very Excited That It Can Track Everything Phone Users Do and Sell That to Whoever Is Interested*, FORBES (Oct. 17, 2012), http://www.forbes.com/sites/kashmirhill/2012/10/17/verizon-very-excited-that-it-can-track-everything-phone-users-do-and-sell-that-to-whoever-is-interested/ (reporting "Bill Diggins, one of the Verizon Wireless execs in charge of Verizon's new Precision Marketing Insights, which has the enviable role of selling information about Verizon customers' location, Internet browsing, and app use—'anonymized and aggregated'—to anyone who wants to buy it").

Privacy invasions are not limited to new personal devices or the Internet. Even television is moving to targeted advertising through cable boxes.[54] Cable companies will go so far as to match names and addresses of subscribers with data, or take data on television viewing and match it with household data.[55] Other companies regularly swipe licenses, collecting all the information contained on them which they later sell.[56] Private entities are chipping away at privacy in every aspect of daily life.

c. Cloud computing

Additionally, many people or businesses store documents or information through "cloud computing."[57] Were these documents or pictures to be reviewed by law enforcement in hard copy, a warrant would be necessary. However, the legal framework that protects privacy in electronic communications, the Electronic Communication Privacy Act (ECPA),[58] allows access to such documents with far less than a warrant.[59] As commercial entities migrate storage to the cloud, consumers are forced to store their information at that location.

3. Privacy Intrusions By Third Party Takers

Even more insidious than primary party takers are third party takers, completely unknown to the users. Several commercial entities obtain information about individuals in a variety of ways, and then sell it to other companies, the advertising industry, or even campaigns.[60] These methods are as broad as primary party takers. However, they deserve separate attention so as to demonstrate the gravity of the

---

54. Jessica E. Vascellaro, *TV's Next Wave: Tuning in to You*, WALL ST. J., Mar. 3, 2011, at A1; Stephanie Clifford, *Cable Companies Target Commercials to Audience*, N.Y. TIMES, Mar. 3, 2009, at B1; Tim Arango, *Cable Firms Join Forces to Attract Focused Ads*, N.Y. TIMES, March 10, 2008, http://www.nytimes.com/2008/03/10/business/media/10cable.html.

55. Vascellaro, *supra* note 54.

56. Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data For Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595, 627 (2004).

57. "The 'cloud' [is] a purely abstract concept, originating in the presentation representations of the Internet and networks for many years. The cloud comes into existence when one or more cloud services is delivered to one or more customers." *Risk Management Glossary C*, COWENS RISK SOLUTIONS, http://cowensrs.co.uk/glossary_c.html (last visited Apr. 18, 2013) (sharing Gartner, Inc.'s defitition). Cloud computing is "a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies." *IT Glossary: Cloud Computing*, GARTNER, INC., http://www.gartner.com/it-glossary/cloud-computing/ (last visited Apr. 18, 2013).

58. At the time of publishing, proposals to amend ECPA were being discussed in Congress, but the proposals remained dormant at the close of the 112th Congress.

59. *See* STEVENS, *supra* note 27, at 12.

60. *How You Can Be Tracked Online*, ABINE, http://www.abine.com/tracking.php (last visited Nov. 29, 2012) (finding data companies "track you to provide targeted advertising, classify you into a demographic group, and resell information about you to other companies. Similar to mail-order catalog companies that sell and re-sell your name, address, and phone number to others trying to sell you related products"); *see* Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL ST. J., Oct. 24, 2010, at A1 (explaining how one prominent data tracking company was the first such company to actually know and use individuals' names from data research); *see also*, Natasha

invasion. It is one thing to accept that entities with whom individuals choose to interface collect data, but it is quite another matter when the individual has no knowledge of the entity at all.

a. Computer based intrusion

Unbeknownst to the user, these third party takers install cookies on the users' computer, and these cookies both obtain details about the user and transmit them to others.[61] Privacy concerns arise not only due to the taking of information, but also its subsequent uses. These third party takers "surreptitiously" track users' actions and then segment the data into hundreds of categories, cross-referencing it with other information, including age, political affiliation, gender, household income, and marital status.[62] That invasion is remarkable. For example, an individual interfaces with an entity and uses his email address to sign on or become a member. That company sends the email address to an online tracking company, who then installs a cookie on the individual's computer to track private information. While users are generally aware that much is tracked online and they cannot control it, this specific placing of items on their computer to track them occurs unbeknownst to the user.

Although the entities claim this data is anonymous, it often is not.[63] Many of these companies acknowledge they collect such information, but claim that they do not sell names to their clients.[64] However, some companies concede they will send personal information to a campaign or company that already has the email address of the individual.[65] This fictional anonymity was illustrated by the Wall Street Journal's coverage of banks' use of such information. A user arrives at a bank's homepage and the third party "instantly scans the information passed between the person's computer and the web page which can be thousands of lines of code containing details of the user's computer."[66] The entity then can identify where the computer is physically located and access its web browsing history through other databases.[67] Although the third party will characterize this activity as anonymous, it is reliable enough that banks make decisions whether or not to loan money based

---

Singer & Charles Duhigg, *Tracking Voters' Clicks Online to Try to Sway Them*, N.Y. TIMES, Oct. 27, 2012, at A16 (explaining how political campaigns have begun using data tracking companies to enlist voters).

61. Elinor Mills, *Behavioral Data Tracking Rising Dramatically (Q&A)*, CNET (June 19, 2012), http://news.cnet.com/8301-1009_3-57456273-83/behavioral-data-tracking-rising-dramatically-q-a/; *see, e.g.*, Steel, *supra* note 60.

62. Steel, *supra* note 60; Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 3, 2010, at A1. Such tracking is also done through the use of cell phones. *See, e.g.*, Hill, *supra* note 53.

63. Steel, *supra* note 60.

64. *Id.*

65. *Id.*

66. Steel & Angwin, *supra* note 62.

67. *Id.*

on this information.[68] The user does not know of this third party taker, nor of the item placed on his computer.

Another method of third party taking is data scraping. These "scrapers" go to a site and use sophisticated software to "scrape" data from the site.[69] While "data" sounds innocuous, this scraping can include copying every message from an online forum.[70] Not only do these entities "harvest online conversations" which can be highly personal (such as fora that concern medical, personal, or financial issues) where users believe they are anonymous; but these entities also "collect personal details from social-networking sites [and] résumé sites."[71] Some then connect the data with real names. For example, the Wall Street Journal series reported on a company seeking a patent that will allow it to "match[] people's real names to the pseudonyms they use on blogs, Twitter and other social networks."[72] Another commercial entity has been documented to have matched data from social networking sites with email addresses, and indexed over 600 million email addresses.[73] This effectively connects databases of information to cookies surreptitiously placed on computers, and combines offline profiles with online tracking.[74] Again, in such situations, the individual may have voluntarily shared very limited information (such as his email address) with a primary party. In so doing, he did not voluntarily share, or even knowingly risk sharing, all that he does both on and offline.

The Federal Trade Commission (FTC) has expressed concern regarding these so-called data brokers and their deceptive practices. One commercial entity allowed customers to pay a fee to opt out of tracking, yet their personal information continued to be available to other companies.[75] Another gained access

---

68. *Id.*

69. Julia Angwin & Steve Stecklow, *'Scrapers' Dig Deep For Data on Web*, WALL ST. J., Oct. 11, 2010, http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html; George H. Fibbe, *Screen-Scraping and Harmful Cybertrespass After* Intel, 55 MERCER L. REV. 1011, 1012–13 (2004) ("Screen-scraping, also called data aggregation or indexing, encompasses technologies variously referred to as robots, spiders, crawlers, or automated devices. Disputes over screen-scraping tend to be between business actors and involve unauthorized access to websites for profit . . . .").

70. *See* Angwin & Stecklow, *supra* note 69; Fibbe, *supra* note 69.

71. Angwin & Stecklow, *supra* note 69; *Escaping the 'Scrapers*, DIGITS WALL ST. J. BLOG, (Oct. 11, 2010, 9:35 PM), http://blogs.wsj.com/digits/2010/10/11/escaping-the-scrapers/ (explaining "the sites gather information from public sources such as property records and telephone listings, and other information is harvested by "scraping"—or copying—websites where people post information about themselves"). For a list of online data brokers and scrapers, see *Online Data Vendors: How Consumers Can Opt Out of Directory Services and Other Information Brokers*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/online-information-brokers-list (last visited Mar. 4, 2013).

72. Angwin & Stecklow, *supra* note 69.

73. *See* Steel, *supra* note 60; *see also*, RAPLEAF, https://www.rapleaf.com/ (last visited Apr. 14, 2013) (advertising others to "instantly get data such as age, gender, and more. Upload a file in any of these supported formats: .xls, .xlsx, .txt, .csv, with any number of email addresses").

74. Steel, *supra* note 60.

75. *In re* Chitika, Inc., No. 102-3087, 2011 WL 914035 (F.T.C. Mar. 14, 2011) (consent order accepted for public comment); STEVENS, *supra* note 27, at 9.

to personal information by selling tracking software to parents so that they could monitor their children's online activity, but then sold the information collected about the children to others.[76] While data-collecting firms gather information from public records, they also conduct surveys to deceive people into revealing information concerning their lifestyle, health, and personal information, ultimately in order to sell it.[77]

The technologies being developed are far more intrusive and sophisticated than just cookies. Beacons, also known as web bugs or pixels, allow the collection of much more personal information. These are "small pieces of software that run on a web page. They can track what a user is doing on the page, including what is being typed or where the mouse is moving."[78] They can capture what a user sees on the web site, including the user's comments or interests, and "package[] that data into profiles about individuals, without determining a person's name."[79] This package is then sold to other companies.[80]

The tracking of users' information is not limited to web site visits or forum information. Deep Packet Inspection (DPI) is another method used by commercial entities. When information is sent and received over the Internet it is done so in packets of information labeled with a header, which indicates where the packet came from and where it is going.[81] DPI documents "every web page visited, every email sent and every search entered. Every bit of data is divided into packets—like

---

76. STEVENS, *supra* note 27, at 8; F.T.C. v. Echometrix, Inc., No. 10CV-5516, 2010 WL 4926541 (E.D.N.Y. Nov. 30, 2010).

77. Angwin & Stecklow, *supra* note 69.

78. Angwin, *supra* note 19; Francoise Gilbert, *Beacons, Bugs, and Pixel Tags: Do You Comply with the FTC Behavioral Marketing Principles and Foreign Law Requirements?*, 11 J. INTERNET L. 3, 4 (2008) (stating that "Web beacons . . . are different from cookies . . . [they]are inconspicuous to the user. They consist of a small string of software code, typically 1-by-1 pixel in size, that is placed on a Web page or an email message to track pages viewed or emails opened"). In the *Wall Street Journal* investigation, a majority of the sites visited placed at least seven beacons from third companies on the user's computer. Angwin, *supra* note 19.

79. *Id.*

80. *Id.*

81. Duncan Geere, *How Deep Packet Inspection Works*, WIRED CO. UK (April 27, 2012), http://www.wired.co.uk/news/archive/2012-04/27/how-deep-packet-inspection-works; Ralf Bendrath, *Global Technology Trends and National Regulation: Explaining Variation in the Governance of Deep Packet Inspection* 10 (2009), http://userpage.fu-berlin.de/bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf. Prior to DPI, Shallow Packet Inspection (SPI) occurred where headers or just a few packets were inspected, usually to prioritize traffic over the Internet or ensure no viruses entered a system. BENDRATH, *supra* note 81. "[Deep Packet Inspection] is the Internet equivalent of the Postal Service reading your mail . . . . ISPs are opening these envelopes, reading their contents, and keeping varying amounts of information about the communications inside for their own purposes." Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1453 (2009) (quoting *Broadband Providers and Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 110th Cong. 15 (2008) (testimony of Gigi B. Sohn, President, Public Knowledge)). It was and it is quicker and more efficient than examining each piece of data. Geere, *supra* note 81. DPI, however, takes this examination to a new level of intrusiveness. It is much more intrusive than cookies or SPI. Cookies count the number of times a user may go to a particular web site, but DPI monitors all activity. Steve Stecklow & Paul Sonne, *Shunned Profiling Technology on the Verge of Comeback*, WALL ST. J., Nov. 23, 2010, at A1.

electronic envelopes—that the system can access and analyze for content."[82]

The purpose of DPI can vary from the objectively reasonable to the nefarious. As with the other technologies previously discussed, the history of DPI reflects a move to the latter. It can be used to filter out malware, to block traffic that will use a great deal of bandwidth, or to block illegal or copyrighted material. It can also be used for government surveillance, censorship (as is done in China), or advertisement injection into websites to match the user's interests.[83] When network providers engage in this it is akin to the letter carrier opening a letter and resealing it.[84] Indeed, network providers have access to a subscriber's identity and web surfing information because they are the ones who transport it. As a result, third party takers offer these providers the DPI service, obtain this information, and then inject advertisements into to the websites the user visits.[85] Initially, when some entities announced an intent to utilize DPI in 2007 and 2008, the United States Congress and the European Union met them with alarm.[86] However, it has made a comeback as of 2010, given the potential profits to service providers for handing over this valuable and unique data: a $20 billion dollar online advertising industry.[87]

b. Device based invasions

Third party inspection is not limited to software, either. "Fingerprinting devices" are another effort of third party takers. It has been reported that some companies are attempting to build a "credit bureau" for devices, which will create a profile for every cell phone or computer. This information will include information on who the user is, his online behavior, demographics, etc.[88] It is created by using the unique data located on a device to identify the user and create a profile for the device which will be sold. This is done by embedding the technology in a web site or app.[89] A user connects to a web site with his email address and the website shares the information with an offline data company which obtains information about the user, strips the name, and sends the information to the "fingerprinting" company which combines that information with the profile it has

82. Peter Whoriskey, *Every Click You Make*, WASH. POST, Apr. 4, 2008, at G01.

83. Geere, *supra* note 81.

84. *Id.*

85. BENDRATH, *supra* note 81.

86. *Id.*; Geere, *supra* note 81.

87. *See* Julia Angwin & Jennifer Valentino-Devries, *Race Is on to 'Fingerprint' Phones, PCs*, WALL ST. J., Nov. 30, 2010, at A1; Whoriskey, *supra* note 82.

88. *Id.*; *see also* Robert Vamosi, *Device Fingerprinting to Fight Real-Time Transaction Fraud*, FORBES, March 17, 2010, http://www.forbes.com/sites/firewall/2010/03/17/device-fingerprinting-to-fight-real-time-transaction-fraud/ (discussing companies such as ThreatMetix which use device fingerprinting methodology to probe beyond mere cookies and browser data to identify the machine being used for online access in order to fight fraud).

89. Angwin & Valentino-Devries, *supra* note 87.

created of the devices.[90] These companies hold onto this data for an unlimited time, and users are never notified by these third companies that their devices are being fingerprinted.[91]

B. Commercial Conditioning and Data Collection is Not Voluntary

Thus far, this article has described this information collection as "involuntary." No doubt commercial entities, whether primary or third party takers, would disagree, pointing to privacy policies. These are the privacy terms, often within a terms of service agreement, dictated to a consumer in exchange for access to the service. The industry would likely argue that, far from being involuntary, such a taking of information is fully voluntary because notice is given to the user that this could happen within the privacy policy. This argument fails both legally and factually.

1. Legally

The concept of voluntariness is one that pervades criminal procedure and is fairly uniformly understood. Two areas where voluntariness is integral include the Fifth Amendment requirement that a statement be voluntary, as well as the Fourth Amendment requirement that consent to search be voluntary.[92] Such situations—making a statement to the police or consenting to a search—are analogous to the activity at issue in this Article. At their essence, a statement to police or a consent to search are *disclosures of information.* The industry defends itself by arguing that data collection is also based on consent. Therefore, the legal principles surrounding voluntariness of these disclosures (statements or searches) are applicable.

The test of voluntariness "remains . . . the only clearly established test in Anglo-American courts for two hundred years . . . ."[93] For a disclosure of information—i.e., a statement—to be voluntary, the disclosure must be "the product of an essentially free and unconstrained choice by its maker."[94] A statement is not such a product if the individual's will was overborne in order to obtain the information.[95] A voluntary disclosure of information cannot be the "result of duress or coercion, express or implied."[96] This determination is made considering all the surrounding circumstances.[97]

---

90. *Id.*

91. *Id.*

92. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 225–26 (1973) (discussing the voluntariness test applied to custodial interrogation); Bumper v. North Carolina, 391 U.S. 543 (1968) (stating "where there is coercion there cannot be consent"); Alexander v. United States, 390 F.2d 101, 109 (5th Cir. 1968) (requiring "careful scrutiny for any 'force or compulsion' which may preclude voluntary choice by the defendant").

93. Schneckloth, 412 U.S. at 225–26.

94. *E.g.*, Degraffenreid v. McKellar, 883 F.2d 68, 1 (4th Cir. 1989) (quoting Schneckloth, 412 U.S. at 225).

95. Schneckloth, 412 U.S. at 225.

96. Schneckloth, 412 U.S. at 248.

97. Schneckloth, 412 U.S. at 226.

Voluntariness cannot be presumed solely because the individual gives a statement or allows a search. Similarly, voluntary information sharing cannot be presumed solely because information has been collected. It must be separately established that such a disclosure was voluntary.[98] Research suggests that voluntariness cannot be established simply by establishing the data collection. The public possesses one of two states of mind, neither of which establishes voluntariness. Either individuals feel a loss of privacy due to commercial conditioning, and they are merely acquiescing to the privacy invasion, or they are ignorant of the level of data collection, because many consumers incorrectly believe that primary takers cannot share information about them with third parties.[99] The first is invalid because "mere acquiescence" is *not* voluntary.[100] The second is also involuntary, because if one does not know information is being taken, one cannot have voluntarily consented to it.

Similarly, involuntary disclosures are not solely the result of physical coercion, but can also result from certain types of misrepresentation[101] or deception.[102] When a person is deceived in obtaining information, the law is murky as to whether his consent is valid, and it often turns on whether the deception was fair.[103] Regarding statements, such a disclosure of information may not be voluntary if law enforcement misrepresents the effect on the individual of failing to disclose the information.[104] It is not considered fair to obtain consent to search for one item and then use that consent to collect something vastly different.[105] Courts have refused to find voluntary consent in such cases because such a practice encourages the use of "a seemingly precise and legal warrant only as a ticket to get into a man's home, and, once inside, to launch forth upon unconfined searches and indiscriminate seizures as if armed with all the unbridled and illegal power of a

98. *E.g.*, *Schneckloth*, 412 U.S. at 234; Bolden v. Se. Pa. Transp. Auth., 953 F.2d 807, 824–25 (3d Cir. 1991) (citing United States v. Mendenhall, 446 U.S. 544, 558–59 (1980)).

99. Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327, 1353 (2012).

100. Bumper v. North Carolina, 391 U.S. 543 (1968).

101. As the Third Circuit notes in the context of statements, "when evidence exists to show . . . that a defendant believed he must consent such evidence weighs heavily against a finding that consent was voluntarily given. And when that belief stems directly from misrepresentations . . . we deem the consent even more questionable." United States v. Molt, 589 F.2d 1247, 1251–52 (3d. Cir. 1978).

102. *See, e.g.*, Colorado v. Spring, 479 U.S. 564, 576 n.8 (1987) (noting in certain circumstances affirmative misrepresentations by the police can invalidate a suspect's waiver to voluntarily speak to police).

103. *See* State v. LaFave, 801 N.W.2d 348 (Wis. Ct. App. 2011) (finding that a defendant asserted that her statements were "'obtained through misrepresentations that overcame her free will to give a knowing, voluntary and intelligent statement and as a result, her statement was not voluntary'" because she "was 'tricked' or police used misrepresentations to cause her to give up [her] . . . rights"); People v. Jefferson, 350 N.Y.S.2d 3 (N.Y. App. Div. 1973) (holding that consent was not voluntary and search violated the Fourth Amendment where officers obtained entry by saying that they were investigating a gas leak).

104. *See, e.g.*, Lynumn v. Illinois, 372 U.S. 528 (1963) (misrepresentation that receipt of financial aid and custody of children was conditioned upon disclosure of information to the police); Spano v. New York, 360 U.S. 315 (1959) (misrepresentation that friend's job was conditioned upon disclosure of information).

105. *E.g.*, People v. Ramirez, 747 N.Y.S.2d 711 (N.Y. App. Div. 2002); Jefferson, 350 N.Y.S 2d 3.

general warrant."[106] The same should be true in the disclosure of information. If a commercial entity obtains information deceptively (say, requiring an email address to sign on but using that email address to collect and aggregate personal information), such data collection should not be considered voluntary. The purpose for the disclosure is wholly different from the collection and makes such a disclosure involuntary.

2. Factually

Privacy policies do not necessarily transform coercive or unfairly deceptive efforts to obtain information into voluntary disclosures. It is well documented that privacy policies are inadequate protectors of the users.[107] Indeed, the Commerce Department's Internet Policy Task Force examined whether commercial data privacy policy advances all the goals of protecting consumer trust in an Internet economy as well as "promoting innovation."[108] It concluded that the "basic element of current consumer data privacy framework, the privacy policy, is ineffective because it is often a lengthy, dense, and legalistic document."[109] One reason they can be inadequate is because they can be written in a way that makes them not truly voluntary agreements to disclose known information for known purposes. This lack of voluntary consent is manifested in numerous ways.

First, they often fail to include notice that the entity with whom the user interfaces takes the user's information and shares it with other specific entities.[110] For example, in 2012 Google announced a plan to integrate data across all its products, claiming it would "better tailor its ads to people's tastes."[111] What it did do was send personal information across all its platforms without any say from the consumer.[112]

Second, even if the language stating the primary taker "may" engage in such activity is present, the language describing that risk may be so deceptive to be

106. United States v. Dichiarinte, 445 F.2d 126, 130 (7th Cir. 1971).

107. *See* Matthew A. Goldberg, *The Googling of Online Privacy: Gmail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web*, 9 LEWIS & CLARK L. REV. 249, 272, n.33 (2005) (discussing the enforceability of websites' privacy Terms of Use); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 588–89 (2007) (noting consumers are not likely to read or understand privacy policies); *id.* at 609 (noting privacy policies often fail to protect consumers but do protect companies).

108. STEVENS, *supra* note 27, at 10.

109. *Id.*

110. FTC, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE 1 (Dec. 2012), http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf ("[M]any apps . . . shared kids' information . . . without disclosing these practices to parents.").

111. Cecilia Kang, *Google Announces Privacy Changes Across Products; Users Can't Opt Out*, WASH. POST, Jan. 24, 2012, at B1.

112. Hiawatha Bray, *Google Policy on Data Brings Privacy Worry*, BOSTON GLOBE, Feb. 24, 2012, at B1.

considered unfair.[113] Private entities draft these contracts in such a way that it is very challenging to determine the entities' view of a given issue.[114] Some companies only vaguely disclose that they are engaged with tracking.[115] For example, *The Washington Post* discussed a test run by Knology, a service provider, regarding a deep packet inspection run on several hundred customers. However, the company's twenty-seven-page customer service agreement only contained a "vague reference" to its tracking system, and consumer advocates questioned whether users were properly informed about such practices.[116] When an Internet service provider mines the information of its user, the FTC advises that at least the broadband provider should notify customers and obtain their consent.[117]

Furthermore, commercial entities sometimes mask their privacy practices and then change them once they have obtained the personal data of users.[118] Privacy agreements or terms of service agreements may possess somewhat more clear language when a user joins a service, but then the entity alters the terms in ways unforeseen at the time of the original agreement. While the data may originally be disclosed somewhat voluntarily under the original terms of the agreement, the unilateral changes to the terms made by the primary taker which change the nature, purpose, and scope of the privacy compromise can make the collection of this information involuntary. The current market binds a consumer to that original disclosure even if the agreement is altered. It is certainly not voluntary and informed if it requires individuals to anticipate unknown future changes not only in the agreement, but in the identity of the other party. Moreover, the consumer is disadvantaged because the primary taker often possesses more knowledge of the financial value of the consumer's data.[119] "In fact, it is the business model of many information-intensive companies to draw the consumer in through the offer of one thing and later counter the offering . . . . The ultimate [outcome] may not be even be foreseeable . . . ."[120] Thus, as Professors Whittington and Hoofnagle argue, once a commercial entity obtains personal information for one purpose from an

113. While Facebook allows users to format privacy settings to supposedly monitor and control disclosure of information, Facebook data use policy states "we also put together data from the information we already have about you and your friends . . . . When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services . . . . We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you" and even still "for information others share about you, they control how it is shared" and a user cannot modify the disclosure settings of others. *Data Use Policy*, FACEBOOK http://www.facebook.com/about/privacy/your-info (last visited Apr. 18, 2013).

114. Whittington &Hoofnagle, *supra* note 99, at 1357.

115. Haynes, *supra* note 107, at 595, 604–05 (discussing various websites who are less than clear in disclosure claims).

116. Whoriskey, *supra* note 82.

117. Stecklow & Stone, *supra* note 81.

118. Whittington & Hoofnagle, *supra* note 99, at 1329.

119. *Id.* at 1341.

120. *Id.* at 1342.

individual, it will use the information in violation of the privacy agreement or alter the agreement for a new use of the information.[121]

For example, in July of 2012 Instagram was a photo-sharing app with 80 million users.[122] In September, Facebook finalized the purchase of Instagram.[123] Three months later, Facebook and Instagram altered the Privacy and Terms of Service (through Instagram's blog) by announcing Facebook had a right to *license* and sell all public Instagram photos users had shared to anyone, and all without any notice or payment to the user.[124] Not only did this announcement contain a mandatory arbitration clause forcing users to waive class action rights, but users had no ability to opt out of the new change (just to leave the service, which only affected future pictures), notwithstanding that they had provided their pictures and data under a very different agreement.[125] While one might argue such photos were initially voluntarily shared with Instagram, the personal data associated with the account or photo likely was not. Yet, Instagram announced, again by blog, that it was changing its privacy policy to share such information with third party takers, including Facebook.[126] This move resulted in a class action lawsuit.[127]

Finally, the terms of use or privacy policy documents themselves, because they condition the use of the service on disclosure of information, can be considered coercive under certain circumstances and, therefore, involuntary.[128] Indeed, once the entity has the users' information, the users may want to terminate the re-

---

121. *Id.* at 1349, n.73.

122. Emil Protalinski, *Instagram Passes 80 Million Users*, CNET (July 26, 2012, 1:28 PM), http://news.cnet.com/8301-1023_3-57480931-93/instagram-passes-80-million-users/.

123. Donna Tam, *Facebook Closes Instagram Deal, Welcomes Its 5B Shared Photos*, CNET (Sept. 6, 2012, 8:36 AM), http://news.cnet.com/8301-1023_3-57507465-93/facebook-closes-instagram-deal-welcomes-its-5b-shared-photos/.

124. Declan McCullagh, *Instagram Says It Now Has the Right to Sell Your Photos*, CNET (Dec. 17, 2012, 9:54 PM), http://news.cnet.com/8301-13578_3-57559710-38/instagram-says-it-now-has-the-right-to-sell-your-photos/.

125. Dan Levine, *Instagram Furor Triggers First Class Action Lawsuit*, REUTERS (Dec. 24, 2012, 2:45 PM), http://www.reuters.com/article/2012/12/24/us-instagram-lawsuit-idUSBRE8BN0JI20121224.

126. Don Reisinger, *Instagram to Start Sharing User Data With Facebook*, CNET (Dec. 17, 2012, 8:04 AM), http://news.cnet.com/8301-1023_3-57559553-93/instagram-to-start-sharing-user-data-with-facebook/.

127. Levine, *supra* note 125. Instagram eventually announced a retreat from the claim it could sell users' photographs, but not all of its controversial charges. Declan McCullagh & Donna Tam, *Instagram Apologizing to Users: We Won't Sell Your Photos*, CNET (Dec. 18, 2012, 2:13 PM), http://news.cnet.com/8301-1023_3-57559890-93/instagram-apologizes-to-users-we-wont-sell-your-photos/.

128. For example, many of the web sites simply state they can change the terms at any time without the consumer's permission. *See e.g.*, YAHOO! TERMS OF SERVICE, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (stating Yahoo! subject to the following Terms of Service ("TOS"), which may be updated by us from time to time without notice to you); *Couchsurfing Terms of Use*, COUCHSURFING INT'L, INC., https://www.couchsurfing.org/n/terms (last visited Apr. 1, 2013); BUSINESS TERMS OF USE (USA), SKYPE, http://www.skype.com/en/legal/business-tou-us/ (last visited Apr. 1, 2013) (stating that Skype reserves the right to modify their Business Agreement at any time and may post the notice on its web site). Some sites offer broad statements such as: "we may disclose your personal information as otherwise permitted or required by law." *See, e.g.*, Whittington & Hoofnagle, *supra* note 99, at 1360; *Online Privacy Policy*, ALLY FINANCIAL, http://www.ally.com/privacy/ (last visited Apr. 1, 2013).

lationship. However, doing so is challenging because the entity possesses their information and is not required to relinquish it or cease selling it.[129] Furthermore, participation in some services are so integral to participation in society that it is inherently unfair to condition their receipt on some forms of mandatory privacy invasions.[130] Many of these services have become the "*new utility*" which is so essential that it is unreasonable to deny service.[131]

With regard to phones and phone applications, there often is no privacy agreement at all.[132] "Smartphone users are all but powerless to limit the tracking. With few exceptions, app users can't 'opt out' of phone tracking."[133] Yet, what is shared, unbeknownst to the user, is the important unique device identifier.[134]

C. The Government Obtains This Information from These Commercial Entities With Less Than a Warrant and Probable Cause

With this massive content of personal information collected by primary and third party takers, it is no wonder that law enforcement would seek access to this information. As Professor Slobogin notes, "[g]overnments that want to know about their subjects would be foolish not to take advantage of this situation, and federal and state bodies in this country have done so with alacrity."[135] Indeed, Professor Ohm predicts law enforcement will soon entirely outsource surveillance to private companies. "Police agencies will begin to abdicate their traditional role as conductor of surveillance, because it will be eclipsed by the powerful new systems of private surveillance . . . . who are . . . ungoverned by the state action requirements of the Fourth Amendment . . . ."[136] The effect of collecting and aggregating this digital information allows law enforcement to access "comprehensive dossier on almost any adult."[137] The American Bar Association, concerned with the fact that "law enforcement seeking evidence of crime in records maintained by nongovernmental institutions is surely among the most important and common investigatory activities" created a task force to develop Criminal Justice Standards on Law

---

129. Whittington & Hoofnagle, *supra* note 99, at 1365, 1568.

130. Hoofnagle, *supra* note 56, at 622 (stating "the shortsighted *Miller* decision does not take into account the reality that individuals need to give their information to third parties in order to participate in society"); Haynes, *supra* note 107, at 619–20 (discussing such contracts as unconscionable). This is not to say all conditions of service are coercive. Some are reasonable and necessary for legitimate and responsible business, good corporate citizenship, or certain compliance with criminal investigations.

131. Hoofnagle, *supra* note 56, at 622; Whittington & Hoofnagle, *supra* note 99, at 1365.

132. *See* Thurm & Kane, *supra* note 43.

133. FTC, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (Dec. 2012), http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; Thurm & Kane, *supra* note 43.

134. *See* Thurm & Kane, *supra* note 43.

135. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 317 (2008).

136. Ohm, *supra* note 51, at 1321.

137. Hoofnagle, supra note 56, at 596.

Enforcement access to Third Party Records.[138]

The examples of government access to this information are several. At times, the government relationship to the information collection is direct. For example, the venture capital arm of the Central Intelligence Agency (CIA) was reportedly among the several investors placing several million dollars into such secret data collection.[139] The government has become involved in the creation of "fusion centers," which are "an amalgamation of commercial and public sector resources for the purpose of optimizing the collection, analysis, and sharing of information on individuals."[140] The government is engaged in large-scale data mining for the purpose of obtaining information on subjects.[141] As recently as 2008 it was reported that the federal government was planning data mining by 52 federal agencies, with a vast majority of these efforts "designed to obtain 'personal data."[142] The FBI has sought to invest in technology that will data mine social networking and open source news websites.[143]

The government's access also occurs indirectly when the government requests or purchases information from primary or even third party takers. This is possible because the entities surreptitiously collect information, create databases, and also cater to and tailor the information to each individual government agency so as to facilitate government use of the data.[144] This catering includes allowing the government to prevent outside entities from knowing what or whom law enforcement is researching.[145]

Some of this information is voluntarily disclosed to the public, and law enforcement is doing what it should do in its mission—namely, to investigate crime. Crime investigation or prevention should not remain in the twentieth

---

138. ABA, LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS STANDARDS 14 (2012).

139. In-Q-Tel, created by C.I.A. director George Tenet, reportedly invested approximately $30 million a year in an Internet startup in Silicon Valley, for the purpose of "provid[ing] venture capital for data-mining technologies that would allow the C.I.A. to monitor and profile potential terrorists as closely and carefully as Amazon monitors and profiles potential customers." Jeffrey Rosen, *Silicon Valley's Spy Game*, N.Y. TIMES, Apr. 14, 2002, at 46; *see also*, Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 908 (2008) (explaining "people simply do not interface with the government in the same ways or with the same frequency as they do with the private sector" and therefore "intelligence agencies find themselves particularly drawn to, and in some respects dependent upon, private data resources").

140. Slobogin, *supra* note 135, at 318 (noting that as of 2008, thirty-eight state and local government fusion centers existed, supported by a million dollars in federal funding).

141. *Id.*

142. *Id.* at 319; *see also* Elizabeth Montalbano, *FBI Seeks Data-Mining App for Social Media*, INFORMATION WEEK, (Jan. 26, 2012), http://www.informationweek.com/government/security/fbi-seeks-data-mining-app-for-social-med/232500552.

143. *See* Montalbano, *supra* note 142.

144. *See* Hoofnagle, *supra* note 56, at 608, 621.

145. *See* Hoofnagle, *supra* note 56, at 612. There are positive reasons not to allow this information to be detected such as not alerting a target he is under investigation. Nonetheless, this sort of permanent cloak is an example of the facilitating government access to privately collected information from primary and third party takers.

century world, as crime itself has moved into the twenty-first century.[146] However, some investigation techniques transcend accessing information voluntarily made public (say, by one's social networking site),[147] or disclosed to other individuals who later shared it with law enforcement.[148] Accessing information taken secretly by primary or third party takers is precisely this, and it is the concern of this Article.

State governments are also actively engaging in such programs as well, due to the vastness of the commercial entities' data and the low cost of obtaining it.[149] The result of this massive amount of information being held by the private sector could be, as Professor Ohm predicts, an evisceration of the Fourth Amendment. This occurs because it will be unnecessary for police to obtain a warrant to retrieve information from a suspect which they can obtain from a private company, and the information will be more comprehensive and accurate.[150] Indeed, Professor Hoofnagle has demonstrated that this is already "big business."[151]

This government access is only the beginning. Within the last decade, political campaigns have become heavily involved in data mining information on voters, so called "microtargeting."[152] While the campaigns claim this is an effort to more acutely target messages, the techniques used are the same as the aforementioned.[153] Acting as primary takers or through third party data mining companies, they install cookies on individuals' computers and devices, track their moves and those of their friends, and match that information with offline data on voter

146. *See* Heather Kelly, *Police Embrace Social Media as Crime-Fighting Tool*, CNN (Aug. 30, 2012, 5:23 PM), http://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html (discussing positive ways in which police utilize social media to dismantle street gangs, interrupt criminal activity, and discover evidence of such); Patience Wait, *Police Make Wide Use of Social Tools*, INFORMATION WEEK, (July 20, 1012 10:30 AM), http://www.informationweek.com/government/information-management/police-make-wide-use-of-social-tools/240004077. For an excellent discussion of data mining by the Government see also Slobogin, *supra* note 135.

147. *See e.g.*, Rocco Parascandola, *New York Police Department Issues First Rules for Use of Social Media During Investigations*, NEW YORK DAILY NEWS, (Sept. 11, 2012, 7:15 PM), http://www.nydailynews.com/new-york/new-york-police-dept-issues-rules-social-media-investigations-article-1.1157122 (detailing the NYPD's approval of investigators using social media aliases to gather evidence).

148. *See* United States v. Meregildo, 883 F. Supp. 2d. 523, 526 (S.D.N.Y. 2012) (finding the defendants "legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted—including sharing it with the Government"); Kelly, *supra* note 146 (discussing a case in which a defendant's friend agreed to give police access to the defendant's private information).

149. *See* Slobogin, *supra* note 135, at 319–20.

150. *See* Ohm, *supra* note 51, at 1321.

151. Hoofnagle, *supra* note 56, at 599–614.

152. *See e.g.*, Sasha Issenberg, *How President Obama's Campaign Used Big Data to Rally Voters: Part 2*, MIT TECH. REV. (Dec. 17, 2012), http://www.technologyreview.com/featuredstory/508851/how-obama-wrangled-data-to-win-his-second-term/.

153. *See* Singer & Duhigg, *supra* note 60 (discussing the use of data tracking programs by the 2012 Presidential campaigns).

registration polls.[154] One company claims to have matched over 600 million cookies with 250 million voters.[155] Future agreements with AT&T and other companies will expand this tracking to individuals' mobile phone devices and IP addresses on television sets.[156]

While this may seem like nothing more than effective campaign tactics, it is arguably different. It is different because at the end of the election, one candidate wins and becomes the government. Thus, in the hands of the government flows a vast amount of information about individuals including their preferences, charitable donations, associates, email addresses, political preferences, voter registration information, etc.[157] Most, if not all, was obtained involuntarily and is now in the hands of the government.[158] While the campaigns claim this is all done anonymously,[159] these claims are eerily similar to those of the companies and advertisers who use this technology, and they are equally as hollow, as companies concede that personal information is sent to campaigns that possess the email addresses of individuals.[160] For example, while companies must acknowledge that this type of work is being done for campaigns, they often refuse to disclose exactly which campaigns are clients. Similarly, the campaigns are often less than clear as to what is collected, how it is done, or who is doing the collection.[161]

---

154. *See* Issenberg, *supra* note 152; Singer & Duhigg, *supra* note 60 (reporting that Obama and Romney campaigns had more tracking devices than some major retailers, as many as ninety-seven combined); Tanzina Vega, *Online Data Helping Campaigns Customize Ads*, N.Y. TIMES, Feb. 20, 2012, http://www.nytimes.com/2012/10/28/us/politics/tracking-clicks-online-to-try-to-sway-voters.html?pagewanted=all&_r=0.

155. *See* Allison Brennan, *Microtargeting: How Campaigns Know You Better Than You Know Yourself*, CNN (Nov. 5, 2012), http://www.cnn.com/2012/11/05/politics/voters-microtargeting.

156. *See id.*

157. *See* Singer & Duhigg, *supra* note 60 (reporting campaigns marry information third party trackers obtain about people with information they have collected about voters including political links shared on social networks); Brennan, *supra* note 154 (reporting that data companies collect or purchase personal information and connect it with public available voter rolls); Vega, *supra* note 153.

158. Lois Beckett, *How Microsoft and Yahoo Are Selling Politicians Access to You*, PROPUBLICA (June 11, 2012, 11:45 AM), http://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access-to-you (reporting Microsoft and Yahoo selling browsing information to campaigns without notice to their customers). As this article was going to press, revelations emerged concerning federal government programs collecting records and data regarding foreign nationals and possibly American citizens. Victor Luckerson, *Prism By the Numbers: A Guide to the Government's Secret Internet Data Mining Program*, TIME, June 6, 2013 http://newsfeed.time.com/2013/06/06/prism-by-the-numbers-a-guide-to-the-governments-secret-internet-data-mining-program/. The complete contours of the programs remain to be learned. Although this appears to be beyond the scope of this article as it suggests programs related to national security, as opposed to purely criminal investigations, the limited public reaction further illustrates that the public has been conditioned by private industry to have a decreased sense of privacy. Adam Nagourney, *In U.S. News of Surveillance Effort is Met With Some Concern But Little Surprise*, N.Y. TIMES, June 7, 2013 http://www.nytimes.com/2013/06/08/us/many-americans-appear-resigned-to-surveillance.html?pagewanted=all&_r=0.

159. Brennan, *supra* note 155.

160. *See* Singer & Duhigg, *supra* note 50.

161. Beckett, *supra* note 158. One of the reasons the data collection is possible is that no single federal law comprehensively protects private information held by private sector. Congress has regulated this information on a sector-by-sector basis and, as a result, information such as private health information and video game rentals are regulated but other information, such as credit reporting, is not. *See also* STEVENS, *supra* note 27, at 7 (explaining

II. COMMERCIAL CONDITIONING HAS A CONSTITUTIONAL EFFECT

Some scholars and courts have wrestled with the challenging reality that government access to third party information poses to the Fourth Amendment. This scholarship is essential to comprehending the implications of this new world order. However, this Article suggests the problem is far more upstream than the government's access to the information. The more central threat to the Fourth Amendment is the commercial conditioning of individuals. It affronts the Fourth Amendment protections in two fundamental ways. First, it precludes individuals from establishing an expectation of privacy by eviscerating each prong of the reasonable expectation of privacy test. Second, this taking and possessing of the information affords the government the ability hide behind third parties (given the Third Party Disclosure Rule). While that may be a valid argument in the context of a voluntary disclosure of information to the public, it cannot be valid when the information is *taken* from the individual rather than consciously and voluntarily shared.

A. Commercial Conditioning Precludes the Ability to Establish an Expectation of Privacy

The Fourth Amendment protects an individual's privacy. The protections of the Fourth Amendment are triggered in two instances: first, when the government is involved in a search or an examination of an area in which one has a reasonable expectation of privacy; or second, when the government engages in a physical trespass of a constitutionally protected area while it is seeking information.[162] The first instance, the *Katz* test, is the relevant test for the modern electronic surveillance at issue in this Article.[163]

As to the former, in order to obtain Fourth Amendment protections, a court must find that (1) the individual exhibited an actual expectation of privacy in the location searched (subjective prong) and (2) that expectation is one that society is prepared to accept as reasonable (objective prong).[164] In *Smith v. Maryland*, the Court acknowledged "[s]ituations can be imagined, of course, in which *Katz'* two-pronged inquiry would provide an inadequate index of Fourth Amendment

---

that personal information privacy is regulated by "a patchwork" of federal and state laws). For a comprehensive discussion of many relevant statutes and the ability of the government to access the information upon request see Hoofnagle, *supra* note 56.

162. *See* United States v. Jones, 132 S. Ct. 945, 952 (2012) (explaining that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, but not *substituted for*, the common-law trespassory test") (emphasis added); Florida v. Jardines, 2013 WL 1196577 (2013).

163. *Id.* at 953 (finding that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis").

164. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

protection."[165] Society, through commercial conditioning has reached such a point.

In *Smith v. Maryland*, the Court referenced circumstances "where an individual's subjective expectations had been *'conditioned' by influences alien to well-recognized Fourth Amendment freedoms*," and concluded that when such has occurred, "subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was."[166] While the Court correctly acknowledged the evisceration of the subjective expectation of privacy would mean the traditional *Katz* analysis was no longer valid, the Court incorrectly assumed the source of such a threat would be the government. Indeed, individuals have been conditioned to believe they do not have expectations of privacy. It has been accomplished, not by the government, but by private entities.

This is demonstrated by reference to the very examples of conditioning discussed in *Smith*. These include: "if *the Government* were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry," and "if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations . . . ."[167] The Court recognized that were these to occur, the individual no longer entertained an actual expectation of privacy[168] and the two-pronged *Katz* analysis would fail. *Katz* is quite clear; not only must an individual claim he *expected* privacy, he must have *demonstrated* such.[169] As Professor Clancy notes, there must be an external or proactive act on the part of the individual to conclusively show he had such an expectation.[170] It may be Katz's closing the door to the phone booth,[171] the placing of personal items in a suitcase,[172] or the sealing of an envelope,[173] but it must be demonstrated.

The Court explicitly recognized, therefore, that Fourth Amendment rights should not be curtailed by *conditioning* individuals to believe they are under

---

165. Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979). In *Smith*, the Court held no search occurred when a telephone company, acting at the request of the police, placed a pen register on Smith's phone, thereby confirming that he was the person placing harassing phone calls to the victim. *Id.* at 742.

166. *Id.* at 740 n.5.

167. *Id.* (emphasis added).

168. *Id.* (emphasis added).

169. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (explaining "a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been *exhibited*") (emphasis added).

170. Thomas K. Clancy, *The Fourth Amendment Aspects of Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 220–22 (2005).

171. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

172. United States v. Chadwick, 433 U.S. 1, 13 (1977).

173. *Ex parte* Jackson, 96 U.S. 727, 732 (1877).

intrusive or constant surveillance.[174] Doing so precludes individuals from establishing they have been subjected to a search. Therefore, it precludes them from Fourth Amendment protections. It is important to distinguish here between the general and the specific. Individuals are aware *in general* that commercial entities are surveilling and tracking them. They learn it from unsolicited emails, unrequested advertisements, and references to prior purchases. Thus, commercial conditioning occurs in a *general* sense because individuals know in general they are being tracked. In a *specific* sense, however, they did not know exactly *who* took their information or when their information was taken. This also decreases privacy expectations because they cannot register an objection to the specific taking to demonstrate their privacy expectations.

When commercial entities take information from individuals without their knowledge, by placing devices on their computers to track where they move their "mouses" on web pages, or by engaging in an inspection of the contents of email before it even arrives at the box of the recipients, individuals never have the opportunity to demonstrate an expectation of privacy in this information. If an individual cannot have such an opportunity, then she can never establish a subjective expectation of privacy and, therefore, can never attain Fourth Amendment protections when the government subsequently obtains the information.

Commercial conditioning has a similar effect on the objective prong of the test. This effect exceeds what is done on the individual level. This ubiquitous presence of surveillance, combined with the individual knowledge that there is nothing one can do to prevent it, leads society to feel there is no actual privacy. Thus, there is no privacy expectation one could conclude society would find reasonable. This notion that people feel little if anything is private is apparent.[175] As Professor Brenner notes, a significant effect of this ubiquitous surveillance

> has been a serious reduction in an individual's rights and expectations of privacy. It has become increasingly common for data about transactions and ourselves (Data) to be collected and retained by third parties (Collectors) who often disclose more intimate details of our lives and lifestyles than would have ever been imaginable or acceptable just a decade ago. In turn, this

174. One could argue not all of society understands the level of surveillance and, therefore, is conditioned to believe there is no privacy. As Professor Slobogin has noted, it is difficult to establish actual expectations of society. Nonetheless, under either circumstance, the first prong is impossible to establish. Either the individual believes nothing is private, and fails to claim privacy, or the individual is unaware of the data collection so cannot *demonstrate* a privacy expectation. Christopher Slobogin and Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted By Society,"* 52 DUKE L.J. 727 (1993).

175. Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox, in Ninth Annual Workshop on the Economics of Information Security (WEIS)*, at 3 (2010) (concluding that individuals' ability to publish their information increases their comfort level in privacy and paradoxically leads them to share more such information), http://www.futureofprivacy.org/wp-content/uploads/2010/07/Misplaced-Confidences-acquisti-FPF.pdf; Slobogin, *supra* note 135 at 336; *see also*, Hoofnagle, *supra* note 56, at 616 (noting that American reaction to Choicepoint selling data to the government is less intense than in other countries).

> retention creates an unprecedented risk that a local, state, or federal government (Government) can obtain data, without the need for a warrant, Data about individuals (Consumers) to which it has never had access.[176]

As the practice becomes more common and more challenging for individuals to detect and stop, society risks becoming resigned to a lack of privacy—or "conditioned" to it.

B. Commercial Conditioning Further Eviscerates the Fourth Amendment By Providing the Government a Path Around Fourth Amendment Protections

The final way in which commercial conditioning has weakened Fourth Amendment protections is the imprecise invocation of the Third Party doctrine. This doctrine is generally cited for the proposition that information obtained by the government from the hands of a third party is not protected by the Fourth Amendment.[177] As will be discussed *infra*, such a reading of the doctrine is oversimplified.[178] Nonetheless, this broad invocation of the doctrine can lead only to one conclusion: commercial conditioning makes it impossible to gain the protection of the Fourth Amendment. Professor Ohm convincingly argues that the surveillance of individuals by private entities has done "something important that no FBI lab could ever hope to do—convince the surveillance targets of the world to consensually adopt their surveillance technologies, acting as a neat end-around circumventing the Fourth Amendment."[179]

This is the additional method by which commercial conditioning deteriorates Fourth Amendment protections. Commercial entities defend their actions in part based on the fact they are not the government. In doing so they distort the protections the Constitution provides. That is to say, even when an individual can establish information has been taken without her knowledge or voluntary consent by the entity and delivered to the government, these commercial entities reject the claim of privacy invasion by noting the Fourth Amendment does not apply to them. Doing so further conditions individuals to believe there is nothing they can do to prevent the government from obtaining this information.[180]

---

176. Brenner & Clarke, *supra* note 14, at 212.

177. The Third Party Doctrine asserts that the Fourth Amendment allows "the obtaining of information revealed to a third party and conveyed by [the third party] to Government authorities . . . ." United States v. Miller, 425 U.S. 435, 443 (1976).

178. *See infra*, Part IV (attempting to refocus the broad language of the Court in *Miller* and subsequent interpretations of the Third Party Doctrine to simply embrace voluntary consent to third party use of private information).

179. Ohm, *supra* note 51, at 1322; *see also* Slobogin, *supra* note 135, at 341 (asserting "the Supreme Court's current hands-off approach to record searches cannot justifiably be applied to data mining if societal views about privacy expectations are taken seriously").

180. As previously mentioned, I have argued elsewhere that statutory protection from the commercial removal of this information would protect individuals from the initial privacy invasion. However, in the absence of such congressional action, this use of constitutional jurisprudence remains an option.

By stripping individuals of their ability to demonstrate their subjective expectation of privacy, and by stripping society of its ability to find an expectation reasonable, commercial entities have become the "influence alien to Fourth Amendment freedoms" of which the Court warned. Just as the Court has forbidden the Government from conditioning society to believe it has no privacy, the Court should preclude the government from taking advantage of commercial entities' actions by requiring Fourth Amendment protections to adhere to this information when the government seeks to access it. The next Part of this Article will discuss how this can be done.

III. TECHNOLOGY AND THE FOURTH AMENDMENT—A VEXING BUT NOT NOVEL ISSUE

Scholars, the Court, and individual justices have openly raised this issue. The Court has at times simply raised it and left it unresolved.[181] Scholars, on the other hand, have explored some aspects and suggested solutions. This rich body of work reminds one of the analyses of democracy and its flaws: scholarship and the media often put forth excellent criticisms of the current system, but finding a workable and superior alternative is challenging. A review of some current scholarship, the Court's opinions, and Justices' individual commentaries concerning technology reveals three basic points. First, there is a recognition that technological advances can affect Fourth Amendment conceptions. Second, it is understood that these realities call for alterations to the definition of what the Fourth Amendment protects. Third, notwithstanding this agreement, identifying and implementing a new framework has been somewhat elusive.

Recently, many scholars have struggled with the implications of rapidly advancing technologies.[182] My work attempts to build on these well-considered

---

181. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (arguing that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative"); City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) (stating that "[t]he Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment . . . . The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear").

182. Although much of the dialog is fairly recent, others such as Christopher Slobogin, Ric Simmons, and Thomas Clancy have been exploring this issue for some time. Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo's *Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1394 (2002) (discussing how "the dissenters in *Kyllo* rightly pointed out, varying Fourth Amendment regulation of technology on the prevalence of that technology is troublesome, because 'the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available'"); Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139 (2005) (voicing concern "that law enforcement officials can, perfectly legally, gain access" to personal information regarding finances, health, purchases, housing and activities "much more easily than they can search our houses or even our cars"); Ric Simmons, *Why 2007 Is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531 (2007) (examining "the ways in which new technology has enhanced our privacy," and "the effect of new technology on government surveillance . . . ."); *see* Clancy, *supra* note 170, at 195 (addressing the implications of computer data and storage on the Fourth Amendment). This is by no means an exhaustive list.

approaches. However, as will be discussed, the commercial conditioning proposal suggests a closer reading of the history of the voluntariness component of both the reasonable expectation of privacy test and the third party doctrine.

The scholarship in this area is diverse in some respects, but uniform in others. Some propose a radical rethinking of Fourth Amendment doctrine, while others suggest a more incremental approach.[183] Thomas Clancy offers a compelling case that the Court's and scholars' focus on privacy as the interest protected by the Fourth Amendment is misplaced, and that the right protected is the right to be secure from government intervention.[184] In other words, individuals have the right to exclude the government from invading certain aspects of their lives.[185] While discussing the recent resurgence of property as a Fourth Amendment concept in *Jones*, Professor Clancy astutely observes this concept of property is now playing a different role than in the past.

> [P]rior to *Katz*, property was viewed as a protected interest; in *Katz* that view was rhetorically rejected in favor of privacy as a centralizing principle. However, in the wake of *Katz*, the Court quickly returned property to a central role but that role was often obscured by subsuming property into the reasonable expectation of privacy formula. Hence, a property right was a manner in which a person was said to have a reasonable expectation of privacy. Justice Scalia, in *Jones* returned to the pre-Katz view: property is an independent protected right . . . .[186]

In this approach which challenges privacy as the Fourth Amendment's target right, Professor Clancy incisively observes the right of security has been confused with the *reason* for the right to be secure: privacy.[187]

In his analysis, Professor Clancy confirms a fundamental aspect of the commercial conditioning approach: there is a value in the demonstration of privacy. While Professor Clancy does not support the *Katz* test, he argues effectively that in this technological age the right to exclude the government must be *exercised*, and no Fourth Amendment protection is triggered if an individual does not take steps to exclude the government. Commercial conditioning also asserts there is indeed a value to the demonstration of a privacy expectation. It agrees the Fourth Amendment should not necessarily apply to information publicly and voluntarily disclosed by individuals. However, it recognizes that due to commercial conditioning, no opportunity exists for individuals to demonstrate their privacy. Thus, the current test will always fail to find Fourth Amendment protection.

---

183. Those theories discussed herein are not intended to be an exhaustive list, but are offered as examples of some varying approaches.

184. Thomas K. Clancy, United States v. Jones: *Fourth Amendment Applicability in the 21st Century*, 10 OHIO ST. J. CRIM. L. 303, 316 (2012).

185. *Id.* at 318.

186. *Id.* at 310.

187. *Id.* at 316.

Professor Ohm agrees with Professor Clancy that the Fourth Amendment seeks to ensure liberty, and that privacy is a proxy for this value.[188] However, he also recognizes that notwithstanding the many critics of the *Katz* test, no workable new test has been offered.[189] Professor Henderson openly acknowledges the challenges inherit in replacing the *Katz* test, noting that he at first offered a nine factor test which he has now been able to modify to a more workable four factor analysis.[190] Professor Slobogin argues for a proportionality principle based approach.[191]

More recently, some scholarship observes the phenomenon discussed in commercial conditioning, i.e. there is a fundamental shift in privacy due to technology. Professor Ohm argues minor changes to the Third Party doctrine are insufficient to address this changing reality, because such alterations may only address government surveillance, and will do nothing if no privacy exists at all.[192] Professor Brenner notes "Fourth Amendment protection should not vanish simply because advances in technology permit, and to a certain extent make unavoidable, massive data collection and mining that expose consumers to the enhanced risks of a Collector's breach of trust."[193]

The Court's jurisprudence has long recognized technology affects Fourth Amendment conceptions. *Katz* itself was driven in part by the increasing use of the telephone for communication.[194] The Court has narrowed the protections of the Fourth Amendment due to technological changes such as the rise of air travel.[195] It has also enhanced protections when faced with government use of technology to conduct surveillance of the home.[196] More recently, the Court has become

188. Ohm, *supra* note 136, at 1312.

189. *Id.* at 1309, 1311–13.

190. Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 988 (2007); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507 (2005); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 423 (2006).

191. Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1055 (1998).

192. Ohm, *supra* note 51, at 1331.

193. Brenner & Clarke, *supra* note 14, at 214.

194. Katz v. United States, 389 U.S. 347, 352–53 (1967).

195. Florida v. Riley, 488 U.S. 445, 451 (1989) (holding some surveillance from a helicopter does not violate the reasonable expectation of privacy); California v. Ciraolo, 476 U.S. 207, 215 (1986) (finding that observation with the naked eye from commercial flight does not violate a reasonable expectation of privacy).

196. United States v. Jones, 132 S. Ct. 945, 953 (2012) (acknowledging "we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis") (emphasis in original); Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding when "Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search . . . .'").

hesitant to alter fundamental approaches,[197] recognizing the "judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[198] This hesitation to alter fundamental aspects of the Fourth Amendment was on display in the open argument between some justices in *Jones*. While each opinion reflected recognition that technology was affecting privacy, each suggested a different solution. Justice Scalia and the majority proposed a return to a physical trespass approach, Justice Alito suggested a more incremental application of *Katz* but called for a legislative solution, and Justice Sotomayor more aggressively suggested an abandonment of the Third Party doctrine.[199]

Individual justices have recognized the effect of technology on Fourth Amendment conceptions. As far back as 1890 in their seminal article, *The Right To Privacy*, Warren and future Justice Brandeis argued for a redefinition of privacy because of the development of invasive technologies.

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[200]

In their call for a right to privacy, Warren and Brandeis clearly recognized not only that technology alters realities, but that its ability to allow deep invasions of privacy result in pain for individuals.[201]

Justice Brandeis continued this understanding of the effect of technology on privacy throughout his career, noting:

> Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the

197. City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) (observing "Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.").

198. *Id.* (declining to rule on whether one has a reasonable expectation of privacy in text messages).

199. *Jones*, 132 S. Ct. at 953 (applying an 18th-century guarantee against trespassory unreasonable searches, "which we believe must provide *at a minimum* the degree of protection") (emphasis in original); *id.* at 964 (Alito, J., concurring) (arguing a "legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way"); *id.* at 957 (Sotomayor, J., concurring) (arguing third party disclosure doctrine is "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

200. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (citations omitted).

201. *Id.* at 196 (declaring that "modern enterprise and invention have, through invasion upon his privacy, subjected [man] to mental pain and distress, far greater than could be inflicted by mere bodily injury").

> Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[202]

Justice Brandeis offered more than just a Pavlovian resistance to technological surveillance. Rather, he understood the basic protection from government intrusion into the personal life the Fourth Amendment offered.[203] Indeed, as Professor Brenner notes, the "eventual adoption by virtually every U.S. state of the Warren-Brandeis analysis demonstrates that such a redefinition was an essential consequence of the evolution of these particular technologies."[204]

More recently, Justices Sotomayor and Alito openly discussed not only technology's effect on privacy in general, but on the expectation of privacy analysis specifically. For Justice Sotomayor, the concern is not only the collection of the data, but the aggregation of the data, and the potential for government abuse:

> [T]he Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that . . . making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[205]

Justice Sotomayor would consider the effects on speech of the collection of data as well as its aggregation when evaluating the existence of a reasonable societal expectation of privacy.[206] This would, in turn, lead to asking "whether people reasonably expect that their [activities] will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[207]

IV. THE PROPOSAL: LIMIT THE EFFECT OF COMMERCIAL CONDITIONING BY APPLYING FOURTH AMENDMENT PROTECTIONS TO THIS INFORMATION

This Article shares the recognition that technology affects Fourth Amendment protections, but shifts the issue away from a focus on government surveillance. Commercial conditioning has eroded Fourth Amendment protections, and a judicial solution focused on this central problem is needed.

Identifying the current difficulty and offering a superior solution are two distinct endeavors, and the latter proves to be imperfect no matter what solution is

---

202. Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

203. Warren & Brandeis, *supra* note 200, at 220 (noting the law recognizes a man's house is his castle and asking "[s]hall the courts thus close the front entrance . . . and open wide the back door to idle or prurient curiosity?").

204. Brenner & Clarke, *supra* note 14, at 218–19.

205. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (citations omitted).

206. *Id.* (noting "awareness that the government may be watching chills associational and expressive freedoms").

207. *Id.*

proposed. This Article proposes neither a radically new Constitutional test for privacy or security, nor does it accept the status quo. In the absence of a more practical legislative solution, courts must address commercial conditioning.[208] Our jurisprudence should reflect the kind of privacy promised by the Fourth Amendment.

This proposal has some defining components. First, it does not cover all private information. Instead, it focuses on a narrow portion of the digital dossier: information taken from individuals involuntarily. Next, rather than a new test, this Article proposes courts reinvigorate what is already present in Fourth Amendment protections: the concept of voluntariness.

By reinvigorating voluntariness into the search jurisprudence and the Third Party doctrine, this proposal suggests only a minor adjustment in current law. Moreover, it establishes state action not at the initial collection, but instead at the time the state seeks to access the information from the taker. When the government, in a criminal investigation, obtains information that was taken involuntarily through commercial conditioning (either unknowingly or without meaningful voluntary consent), it must be considered a search by the government, and some Fourth Amendment protections apply. The government should be required to comply with some form of procedural protections.[209]

A. The Purpose of the Fourth Amendment Includes an Element of Voluntariness in Information Disclosure

Although the Founders were concerned with the government engaging in abusive home searches, it has long been understood that the Fourth Amendment's protections encompass more majestic concerns as well. "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence . . . ."[210] Rather, the Founders noted the essence of the offense was the invasion into one's personal and private rights.[211]

Central, although not exclusive, to one's personal and private life is one's papers. Quoting from Lord Camden's condemnation of general warrants, the Court has noted "papers" are the owner's "dearest property."[212] Eighteenth century general warrants aimed at the "discovery . . . of books and papers that might be used to convict their owner[s]" were certainly "in the minds of those who framed

208. Mary Leary, *supra* note 2, at 347.

209. These procedural protections do not necessarily mean probable cause. A full warrant is not required for every government request of information. Modern Fourth Amendment jurisprudence recognizes that the "central inquiry" of the Amendment is reasonableness. Terry v. Ohio, 392 U.S. 1 (1968). Probable cause has been seen as a flexible concept in which courts consider the nature of the inquiry and balance the intrusion against the government's justification. *E.g.*, *Terry*, 392 U.S. 1, Camara v. Mun. Ct. of City & Cnty. of S.F., 387 U.S. 523 (1967). This balance is for courts to determine.

210. Boyd v. United States, 116 U.S. 616, 630 (1886).

211. *Id.*

212. *Id.* at 627–28.

the Fourth Amendment to the Constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures."[213]

The concern was arguably more specific than that. Lord Camden in 1765, and the Court in 1886, were not only concerned with access to one's personal papers, but specifically with a coercive removal of said papers. "[A]ny *forcible* and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime . . . is within the condemnation of [Lord Camden] . . . [and is] the true doctrine on the subject of searches and seizures . . . ."[214]

Boyd is an early comprehensive treatment of the scope of the Fourth Amendment, and it gave the Fourth Amendment a decidedly liberal interpretation—focusing on property rights as those which define the boundary between reasonable and unreasonable searches and seizures. Although *Olmstead v. United States* largely undercut *Boyd* by limiting Fourth Amendment protections to papers, houses, and effects, *Katz* reversed that aspect of *Olmstead* and found intangible conversations also protected by the Fourth Amendment.[215] In so doing, the Court made some important observations. First, government access to certain intangibles such as thoughts, conversations, or actions done in private are apparently an extension of the person. Second, it matters whether the person voluntarily shared the information contained in the tangible and intangible sources, or whether another entity simply took information.

This is consistent with Warren and Brandeis' approach in which they discussed as central to the concept of privacy the right to freely determine what information about oneself is shared. "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[216] While one might be tempted to argue this does not extend to transactional information on the Internet, Warren and Brandeis were clear that the right to limit the publication of such information "does not depend upon the particular method of expression."[217] They specifically demanded that any individual consent to disclosure of information he deems private. "[T]he individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent."[218] They specifically state the right ends only when the individual himself publishes the information or it is done by a third party with the consent of the

213. *Id.* 625–27.

214. *Id.* at 630 (emphasis added).

215. Katz v. United States, 389 U.S. 347, 353 (1967); Olmstead v. United States, 277 U.S. 438, 457, 464, 466 (1928).

216. Warren & Brandeis, *supra* note 200, at 198.

217. *Id.* at 198–99.

218. *Id.* at 199.

individual.[219]

Not only was the idea of consent to publication a component of the early understanding of the Fourth Amendment protections, but some have written the Amendment also has roots in concerns regarding private intrusion as well. Professor Brenner argues the Fourth Amendment's origin was initially prompted by English laws concerned with trespass from private entities.[220]

Whether one's touchstone for the Fourth Amendment is property as in *Boyd*,[221] privacy as in *Katz*, or security as argued by recent scholars,[222] the individual retains the autonomy to decide what is private (or secure) and what is public and unprotected. *Katz*'s use of the subjective prong speaks to the importance of the individual determining what is private.[223] Indeed, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[224] Thus, meaningful voluntary consent to disclose information is relevant to the privacy inquiry.[225]

B. This Re-Invocation of the Voluntariness Aspect of Fourth Amendment Protections is also Consistent with the Third Party Doctrine

The Third Party doctrine (and to a lesser degree, the Assumption of Risk doctrine) as they are currently understood, may at first appear to preclude this proposed solution.[226] It is such an obstacle that many scholars and judges,

---

219. *See id.* at 218 (asserting that "[t]he right to privacy ceases upon the publication of the facts by the individual, or with his consent").

220. Brenner & Clarke, *supra* note 14, at 234–37 (noting that fifteenth century kings and parliaments began authorizing trade guilds to search others' workmanship, a practice which was followed by star chamber courts authorizing searches directed at individuals for libel, and finally, general warrants).

221. *Jones* also invoked property as a touchstone. *See* United States v. Jones, 132 S. Ct. 945, 951–52 (2012) (stating that under *Katz* alleged Fourth Amendment seizures must be placed in reference to concepts of real or personal property or to understandings that are recognized and permitted by society).

222. Professor Clancy's approach, which abandons privacy as the touchstone of the Fourth Amendment in exchange for security, requires an individual to take steps to exclude the government "consistent with the Supreme Court's view that voluntary exposure to the public eliminates Fourth Amendment protection." Clancy, *supra* note 184, at 320.

223. That is not to say the reasonable expectation test is subjective. While the individual must demonstrate a subjective expectation of privacy, such is necessary but not sufficient to establish a reasonable expectation.

224. Katz v. United States, 389 U.S. 347, 351–52 (1967) (citations omitted).

225. A voluntariness framework is not without drawbacks. Voluntariness analysis is not a bright line test, to be sure. While ambiguities will occur, it is a superior analysis than the current approach, which leaves all information obtained by primary or third party takers unprotected.

226. These doctrines are often treated synonymously. Although related, they are distinct. Ten years before the articulation of the Third Party doctrine, the Court held in *Hoffa v. United States*, 385 U.S. 293 (1966), that statements of the defendant made to a government informant were not protected by the Fourth Amendment. In so doing the Court asserted that the defendant "assumed the risk" that any information gleaned would be shared with the authorities. Therefore, the assumption of risk doctrine technically applies to what individuals disclose to other people. *United States v. Miller*, 425 U.S. 435, 440 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), are the cases which are considered to be the origination of the Third Party doctrine. Their logic embraced the assumption

including most recently Justice Sotomayor, have questioned the Third Party doctrine's utility in today's age of information exchange:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[227]

However, a close examination of this doctrine indicates an inherent voluntary consent aspect to it. By reinvigorating the voluntariness component, such a radical step of eliminating the Third Party doctrine could be unnecessary.

The most commonly cited description of the Third Party doctrine is the following quote from *United States v. Miller*, in which the Court ruled the defendant possessed no Fourth Amendment interest in bank records the government obtained through a subpoena.[228]

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[229]

This is admittedly language of breadth. However, the focus on this one sentence in *Miller*, so often repeated in later cases as the complete Third Party doctrine, seems to be an overly broad view of the doctrine itself or, at least, its original intent. The Third Party doctrine can be understood to contain an implied requirement of voluntary consent[230] to disclosure of information. This is supported by *Miller* factually and legally.

Factually, *Miller* addressed information the defendant was completely aware he

---

of risk analysis, but embarked on a slightly different approach addressing information individuals disclose to other entities. *E.g.*, Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1100 (2006).

227. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

228. United States v. Miller, 425 U.S. 435, 440 (1976).

229. *Id.* at 443.

230. Professor Kerr, in his defense of the Third Party doctrine, has argued even further that the doctrine should be understood as a consent doctrine. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 565 (2009). *But see* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 44 (2011) (arguing that the Third Party doctrine has been unpopular as state constitutional law and its rationale cannot keep pace with technological change). While this Article does not embrace the doctrine with the same vigor, it is worth noting other scholars have recognized an even more expanded understanding of voluntary consent within its meaning.

shared because he affirmatively and voluntarily did so. The Court focused its assessment on the lack of a legitimate expectation of privacy in "original checks and deposit slips" since

> [t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained . . . contain *only information voluntarily conveyed to the banks and exposed to their employees* in the ordinary course of business.[231]

These types of documents—written checks or deposit slips—have a knowing and voluntary aspect to them. The consumer must physically fill them out, sign them, hand them to a person (or today put them in a machine). The consumer knows a person must eventually review the document because it is a necessary record for the transaction. Indeed, the consumer himself receives a receipt and later a statement documenting the transaction. The consumer wants this record created in order to establish that he made the deposit or withdrawal. At the time of the disclosure, the consumer possesses two critical pieces of information. He knows *not only* that the information *is being shared* but that *the content* of the shared information because he himself disclosed it.

This is distinct from the knowledge a consumer has when a primary taker or third party taker installs a super beacon on her computer. The consumer knows neither the beacon is retrieving information from her computer *nor* the content of the information obtained.

The *Miller* legal analysis also demonstrates a voluntary component as it specifically mentions this information is not protected because it was "*voluntarily* conveyed" to the third party.[232] This is entirely different from the information taken from consumers at issue in this Article, i.e., information taken by the primary party without obtaining meaningful consent or even without informing the consumer or information taken from the consumer by third party takers unknown to him. As Justice Sotomayor observes,

> I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.[233]

While Justice Sotomayor suggests a reevaluation of the Third Party doctrine in the "digital age," such a drastic approach may not be necessary if the doctrine were returned to its original scope: a doctrine that announces a lack of protection for information knowingly and voluntarily disclosed to the public.

---

231. *Miller*, 425 U.S. at 442 (emphasis added).

232. *Id.* (emphasis added).

233. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

The doctrine's difficulty in adapting to modern times is grounded in its overbroad interpretation, and results in equally overbroad power by the police to invade privacy. Professor Brenner has observed the current understanding of the related Assumption of Risk doctrine is similarly flawed. She argues that it too imprecisely equates the transmittal of data with voluntary disclosure of information to the public.[234] The result, as Professor Slobogin vividly observes, is an ability by the government to circumvent the Fourth Amendment by utilizing private sources.

> The implications of *Miller* and *Smith* for data mining are fairly clear. These cases stand for the proposition that the government can obtain information about us from third parties without worrying about the Fourth Amendment . . . . *Miller* itself relied to some extent on the fact that Miller had "voluntarily" provided his financial information to the bank, leaving open the possibility that situations involving inadvertent disclosure could produce a different result.[235]

Miller cites to *Hoffa*, *Katz*, and *White* as supporting this analysis, injecting the assumption of risk approach into the Third Party doctrine.[236] The citation to these cases further confirms the presence of a voluntary consent aspect to both doctrines. In *Hoffa*, the Court found no Fourth Amendment protection for conversations that the defendant shared with an informant. The Court observed that the reason for this holding was "every conversation which he [the informant] heard was either directed to him or *knowingly* carried on in his presence."[237] Although the Court held the defendant cannot claim a privacy interest based on the "wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it," central to that conclusion was the *voluntary* nature of the disclosure. In *Hoffa*, as in *Miller*, the defendant possessed those two critical pieces of information; he knew *both* that he was disclosing information and the *content* of that information. This is distinct from information taken by commercial entities without the consumer's knowledge or consent.

Miller also referred to *Katz* for its articulation of the Third Party doctrine, and *Katz* supports a re-insertion of a requirement of knowing and voluntary consent to disclosure. *Katz* states explicitly "[w]hat a person *knowingly* exposes to the public . . . is not a subject of Fourth Amendment protection."[238] Katz shared information with the person on the other end of his telephone call. As in *Hoffa*, had the other participant shared that information with the police or anyone else, Katz

---

234. Brenner & Clarke, *supra* note 14, at 246.

235. Slobogin, *supra* note 135, at 330.

236. United States v. Miller, 425 U.S. 435, 440 (1976) (quoting Hoffa v. United States, 385 U.S. 293, 301–02 (1966)) (agreeing there is no Fourth Amendment violation "unless there is an intrusion into a zone of privacy").

237. Hoffa v. United States, 385 U.S. 293, 302 (1966) (emphasis added).

238. Katz v. United States, 389 U.S. 347, 351 (1967); *see Miller*, 425 U.S. at 442 (finding personal checks exposed to a bank and its employees does not retain a defendant's justifiable right to privacy).

would have no Fourth Amendment claim because he had assumed the risk this would happen. He knew he was disclosing information to the other participant of the conversation, and he knew the content of that information. However, the *Katz* Court did not find this meant he risked a third party (in this case the government) taking the information from him without his knowledge or consent. That was not among the risks he assumed, nor did his disclosure of the information function as information "exposed to the public."

A case frequently associated with *Miller* for the Third Party doctrine is *Smith v. Maryland*,[239] in which the Court held people do not have a reasonable expectation of privacy in the numbers that they dial into their telephones. The Court further held the use by the Government of a pen trap and trace device, therefore, did not demand Fourth Amendment protection. Central to the Court's analysis was the fact that, as the majority saw it, people "know that they must convey numerical information to the phone company . . . and that the phone company does in fact record this information for a variety of legitimate business purposes."[240] Not only was it critical that the defendant's disclosure was somewhat knowing, it was also made using free will. "[A] person has no legitimate expectation of privacy in information he *voluntarily* turns over to third parties."[241]

This division between what is protected by the Fourth Amendment and what is not is of course somewhat unclear, but part of this fault line appears to include knowing information is being revealed, as well as knowing the content of said information. Professor Ohm describes the development of the Fourth Amendment in two camps, with the "assumption of risk" doctrine of *Miller*, *Hoffa*, and *Smith*, and the "knowing exposure rule" reflected in *Katz*, *Knotts*, *Dow*, and *Ciraolo*.[242] This is not only an accurate description of the body of law, but underscores the awareness requirement embedded in the Third Party doctrine. In the assumption of risk cases, one is subjectively aware of the risk the bank teller or phone operator will share the exchanged information. In the Third Party cases that find no expectation of privacy, one knows at least that he has exchanged information available for the government to collect because of his own voluntary and knowing acts. This framework seems fair to the consumer regarding information the consumer directly disclosed knowingly to the primary party. However, it does not seem fair when the consumer does not know what information the taker is collecting or even that it is actually collecting it. It is even more nefarious when one is unaware of *the existence* of the third party taker let alone that it is taking information.

Another aspect of this voluntary exposure is the purpose of the information exchange. Users understand the primary party needs the information for the

239. Smith v. Maryland, 442 U.S. 735, 741–43 (1979).
240. *Id.* at 743.
241. *Id.* at 743–44.
242. Ohm, *supra* note 51, at 1326–28.

functionality of the service they are obtaining. That is consent. However, consent can be for a limited purpose. Users do not necessarily consent to the use of that information for any purpose, such as collection and aggregation.

C. This Proposal is Also Consistent with the Requirement of State Action

A simple response to commercial conditioning could be to call for the illegality of data collection. This Article does not do so as its focus is not data mining per se. Rather, this Article seeks to highlight insidious effects of commercial conditioning on Fourth Amendment protections. As a solution to these detrimental effects, this proposal focuses on the narrow subset of information that is taken from individuals without voluntary consent. When the government seeks to access this information from either primary or third party takers, this Article proposes it must comply with the procedural requirements of the Fourth Amendment.[243] The government should not be allowed to hide behind the Third Party doctrine to prevent this procedural protection, notwithstanding that the initial collection was done by a private entity.

That the Fourth Amendment was created as a limit on government invasions of privacy, as opposed to invasions by private citizens, there can be no doubt.[244] Therefore, when a private entity "unconnected with the government" wrongfully takes information from an individual and the government lacks any knowledge of the seizure, no Fourth Amendment violation occurs.[245] While this may be reasonable in an isolated incident, such as a confidential informant offering a tip to the police, this narrow timeframe of state action is too limiting. The state action occurs when the state contacts the primary or third party taker for the information. The Fourth Amendment is intended to protect individuals from unreasonable searches and seizures. If it would be unreasonable for the government to obtain it from a suspect's effects directly, it is just as unreasonable when the government obtains it from the entity whose business it is to take such information from the suspect and sell it.

Commercial conditioning is distinct from a confidential informant. It is not an isolated incident caused by an individual, as is the case with an informant's tip. As discussed *supra*, the government benefits from the long term collection and aggregation of data by access to it, and at times even purchasing it or financially investing in its collection.[246] Justice Brandeis recognized:

---

243. Of course, courts may determine more specific procedural requirements on a situation by situation basis when balancing the level of intrusion and governmental interests involved. *See e.g.*, Terry v. Ohio, 392 U.S. 1, 27–28 (1968).

244. Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (noting the Fourth Amendment's "origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies"); Barnes v. United States, 373 F.2d 517, 517 (5th Cir. 1967) (holding the Fourth Amendment only proscribes government action).

245. *Burdeau*, 256 U.S. at 475–76.

246. *See supra* Part I (discussing, for example, the increased government use of computer data to thwart terrorism).

> [One] cannot believe that action of a public official is necessarily lawful, because it does not violate constitutional prohibitions and because the same result might have been attained by other and proper means. At the foundation of our civil liberty lies the principle which denies to government officials an exceptional position before the law . . . . Respect for the law will not be advanced by resort, in its enforcement, to means which shock the common man's sense of decency and fair play.[247]

As discussed *supra*, this is third method through which commercial conditioning erodes Fourth Amendment protections. Commercial entities take information without knowledge or meaningful voluntary consent. When the entities are criticized, they respond that their activity is permissible because these entities are not the state. Then they provide the information to the state without any warrant, and at times at a price. When an individual then turns to the state for recourse, the state can argue the actions are permissible because it obtained it not from the individual, but from a private entity. It has been argued that the Fourth Amendment has roots in the prevention of government condoned civilian invasions of privacy as well as governmental ones.[248] It seems reasonable, therefore, that it protects individuals from a surveillance system in which commercial entities take this information without knowledge or voluntary consent of the individuals and make it available to the government either for purchase, mining, or procedures less cumbersome than a warrant.[249] When doing so, these entities function as "forces alien to . . . Fourth Amendment freedoms."[250] The government should not be allowed to utilize such force without some compliance with the Fourth Amendment.

Professor Brenner discusses how such an approach is actually an effort to circumvent the Fourth Amendment, rather than a useful limit to its over-reach. "Allocating the risk to the [c]onsumer gives the [g]overnment an incentive to see that the [c]ollector breaches its agreement with [citizens]; this, in turn, would only encourage [the] [g]overnment to abuse its leverage as a regulator and prosecutor . . . ."[251] Thus, it allows the government to abuse its power without being held accountable. As Professor Hoofnagle notes, "[the] distinction between the risks of government and commercial privacy risk is no longer tenable."[252]

The argument that commercial conditioning is beyond the scope of the Fourth

---

247. *Burdeau*, 256 U.S. at 477 (Brandeis, J., dissenting).

248. Brenner & Clarke, *supra* note 14, at 234–37 (noting fifteenth century kings and parliaments began authorizing trade guilds to search other's workmanship, which was followed by star chamber courts authorizing searches directed at individuals for libel, and finally, general warrants).

249. *See* Smith v. Maryland, 442 U.S. 735, 740–41 n.5 (1979) (stating in situations where an individual's subjective expectations of privacy had been conditioned by "influences alien to well-recognized Fourth Amendment freedoms," a normative inquiry into whether a legitimate expectation of privacy existed is proper).

250. *Id.*

251. Brenner & Clarke, *supra* note 14, at 261.

252. Hoofnagle, *supra* note 56, at 630–33.

Amendment because of the state action requirement can be overcome not by focusing on whether the state originally took the information from the target. Instead it could focus on the action of the government when it *obtained* the information from the commercial entity. If the entity originally obtained the information from an involuntary consumer, the government's attempt to access it is nothing more than the government examining an area in which one has a reasonable expectation of privacy.[253]

While this Article does not claim these private entities act on behalf of the state, when one looks to the reasoning behind "agent of the government" line of cases, one sees support for this proposal. This line of cases finds when a private citizen acts entirely on his own to obtain information illegally, and forwards it to law enforcement without governmental encouragement or knowledge, then the government may use said information, as no state actor has engaged in an unconstitutional search. However, when the government asks, encourages, or knows about such private activity and accepts such information, the private actor is deemed an agent of the state and the action of that person is considered state action.

The Court recognized the importance of "the plain spirit and purpose of the constitutional prohibitions intended to secure the people against unauthorized official action."[254] It cautioned for nearly a century against sanctioning activity that violates the spirit of the protections of the Fourth Amendment:

> The Fourth Amendment was adopted in view of long misuse of power in the matter of searches and seizures both in England and the colonies; and the assurance against any revival of it, so carefully embodied in the fundamental law, is not to be impaired by judicial sanction of equivocal methods, which, regarded superficially, may seem to escape the challenge of illegality but which, in reality, strike at the substance of the constitutional right.[255]

Therefore, it has long been recognized that the Fourth Amendment prohibits not only direct government invasions of privacy, but also situations in which private entities act as "instruments or agents" of the government.[256]

In today's world in which technology is the primary form of surveillance, where many investigations are online,[257] where citizens are under constant video surveillance from public and private entities,[258] where drone use for both commercial

---

253. Professor Ohm has asserted the state action requirement is satisfied at the point the government issues a request. Ohm, *supra* note 51, at 1339.

254. Byars v. United States, 273 U.S. 28, 33 (1927).

255. *Id.* at 33–34.

256. *E.g.*, United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003) (citing Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).

257. Solove, *supra* note 13, at 1084 (explaining "law enforcement agencies have long sought personal information about individuals from various third parties to investigate fraud, white-collar crime, drug trafficking, computer crime, child pornography, and other types of criminal activity").

258. *E.g.*, Cara Buckley, *Police Plan Web of Surveillance for Downtown*, N.Y. TIMES, July 9, 2007, at A1; Steven Kinzer, *Chicago Moving to 'Smart' Surveillance Cameras*, N.Y. TIMES, Sept. 21, 2004, at A18; Jeffery

and government surveillance is developed,[259] and where the government is accessing mined and fraudulently obtained personal data, the line between state actor and private entity is increasingly blurred. In working through these scenarios, courts have looked to two primary factors: (1) whether the government knew of or acquiesced to the private search; and (2) whether the private industry intended to assist law enforcement or had some other independent motive.[260] More than knowledge is demanded, but the government must encourage, initiate, or instigate the search.[261]

Jarrett v. United States is instructive. In *Jarrett*, a computer hacker sent government agents information that a suspect possessed child pornography; the hacker discovered this by installing a Trojan horse on the suspect's computer.[262] While the police were unaware of his action at the time of its occurrence, government agents subsequently exchanged email correspondence with the hacker. They thanked him for his action, stating that if he engaged in the same action in the future, he should "feel free to send" the evidence to them.[263] While the Fourth Circuit concluded thanking the hacker for his investigation after the fact was insufficient to establish state action, "assurance[] . . . that it was interested in furthering its relationship with [the hacker] and availing itself of the fruits of any information that [the hacker obtained]" would be enough even if it did not target a specific individual.[264]

Arguably, society has reached a similar place now. By congressional failure to act,[265] the government's explicit preference for industry growth over privacy concerns,[266] the investment in private entities engaging in this kind of data collection,[267] and the purchasing of the results of this collection for its own archiving,[268] the government has done more than passively accept information from searches of which it is unaware. To the contrary, it has assured these private actors it is interested in such information and has availed itself of its fruits. This could be

---

Rosen, *Protect Our Right to Anonymity*, N.Y. TIMES, Sept. 13, 2011, at A31 (reporting "in 2008, at a Google conference on the future of law and technology, . . . the head of public policy at Google, said he expected that, within a few years, public agencies and private companies would be asking Google to post live feeds from public and private surveillance cameras all around the world . . . anyone with a Web browser would be able to click on a picture of anyone on any monitored street and follow his movements").

259. *E.g.*, Ben Wolfgang, *Bill Would Clip Wings of Private Drone Use*, WASH. TIMES, July 20, 2012, at A01; *The Drone Over Your Backyard: A Guide*, THE WEEK, (June 8, 2012, 9:15 AM), http://theweek.com/article/index/228830/the-drone-over-your-backyard-a-guide#.

260. Jarrett, 338 F.3d at 344–45.

261. *Id.* at 345.

262. *Id.* at 341.

263. *Id.* at 343.

264. *Id.* at 347.

265. The 112th Congress' House and Senate bills regarding Do Not Track legislation, H.R. 654,112th Cong. (2012) and S. 913, 112th Cong. (2012), respectively were referred to committee and made no further progress.

266. *See infra* note 270.

267. Rosen, *supra* note 139, at 646.

268. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

construed as "prior acquiesce or encouragement" of such searches, which has been held to be "implicit approval of all an informant's searches."[269]

While this may seem like a stretch, technology often drives alterations to rules that have been created to ensure that the spirit of the Fourth Amendment is truly fulfilled. This is not new, and was the forcing function of *Katz*, *Ciraolo*, and *Kyllo*, to name a few cases. Commercial conditioning cannot be allowed to facilitate the government access to involuntarily obtained information by wrapping itself in the mantle of a state action defense. To the contrary, this has created a world in which the government will simply privatize its surveillance work, and collect the aggregate data at the end of the process. Commercial conditioning plays a significant role in that process. As a result it must be limited.

Congress thus far has failed to limit government access to information obtained by primary or third party takers. Indeed, under the guise of capitalism, the government has encouraged private entities to do its data collection for it. "The [United States] Department of Commerce recently reiterated that the large-scale collection . . . of [online] personal information is *central to the Internet economy; and that regulation of online personal information must not impede commerce.*"[270] Yet such an approach is perverse to the Fourth Amendment. "Nothing in the history of the Fourth Amendment suggests that citizens should have to choose between their constitutional rights and access to the most efficient means of participating in commercial and personal affairs."[271] Yet, that is exactly where commercial conditioning has taken society.

V. CONCLUSION

The Fourth Amendment is designed to protect individuals from government intrusion into private aspects of their lives. The Third Party and Assumption of Risk doctrines are designed to preclude individuals and suspects who never intended their actions to be private from claiming, after the fact, that they were private. However, as technology has developed, commercial entities have created a world in which the Fourth Amendment cannot protect individuals from government intrusion into their lives. Through their commercial conditioning of society, commercial entities have made it impossible to assert a Fourth Amendment claim in two ways. First they take information from individuals without their knowledge or voluntary consent. In so doing, they preclude the victim from demonstrating a subjective expectation privacy, or one that

269. *See* United States v. Kline, 112 F. App'x 562, 564 (9th Cir. 2004) (citing United States v. Walther, 652 F.2d 788 (9th Cir. 1981) (stating law enforcement's prior acquiescence or encouragement of an informant's search may constitute implicit approval of all the informant's searches, thus making the informant a government agent at all times)).

270. STEVENS, *supra* note 27, at 2.

271. Brenner & Clarke, *supra* note 14, at 262.

society will find reasonable. Second, when the government obtains this taken information, the government hides behind the Third Party doctrine to justify its possession of the information. In essence the government has successfully circumvented the Fourth Amendment protections. The pathway, however, was laid by the commercial entities that facilitate this reality through commercial conditioning.

The only way to restore the protections intended by the Fourth Amendment is to re-invigorate the voluntary consent aspect to privacy protection found in both the privacy cases as well as the Third Party Doctrine cases. These make clear that information obtained from an individual can come in two forms. The first is that which is voluntarily shared by him. The second is that such information was taken from him. Courts must recognize when the government systematically accesses information that was taken from an individual without knowledge or voluntary consent, that individual must be protected. One way to do so is to demand Fourth Amendment procedural protections for the body of information not voluntarily disclosed.